GUIDE ON SEIZING CRYPTOCURRENCIES

GUIDE ON SEIZING CRYPTOCURRENCIES

Version 1.0

Cybercrime Programme Office of the Council of Europe

10 February 2021

This guide was developed within the framework of iPROCEEDS-2
at the initiative of project countries/area
from South East Europe and Turkey

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Acknowledgement

The Guide was prepared in the framework of the Joint Project of the European Union and Council of Europe iPROCEEDS-2, aiming at further strengthening the capacity of authorities in project countries/areas to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet and to secure electronic evidence.

Work on this document was coordinated by the Cybercrime Programme Office of the Council of Europe (C-PROC). All involved experts provided their extensive expertise in drafting this Guide that aims to be a toolbox for investigators all over the world in hands-on activities related to virtual currencies.

Drafted by:

- Christophe LANDRIES (Belgium)
- Jussi AITTOLA (Finland)
- Gergely VESSZOS (Hungary)
- Bart DE VLAMINCK (Belgium)

CONTACT

Cybercrime Programme Office of the Council of Europe (C-PROC)
Tel +33-3-9021-4506
Email alexander.seger@coe.int

DISCLAIMER

This technical report does not necessarily reflect official positions of the Council of Europe or the European Union

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contents

1 Introduction 2

1.1 Rationale 2

1.2 The purpose of the Guide 2

1.3 To whom is the Guide addressed? 3

2 Theory behind seizing 3

2.1 Definitions (FATF/EU) 3

2.1.1 Definition of "Virtual Currency", "Cryptocurrency" and "Virtual Assets 3

2.1.2 Categorization of virtual currencies 6

2.1.3 Definition of "VASP" 7

2.1.4 Definition of Distributed Ledger 8

2.1.5 What is blockchain? 8

2.2 General concepts 9

2.2.1 What is Proof of Work? 9

2.2.2 What is Proof of Stake? 9

2.2.3 What is Yield Farming (in Decentralized Finance)? 9

2.2.4 What is a public-private key pair? 10

2.2.5 What is a wallet? 10

2.2.5.1 Definition 10

2.2.5.2 Custodial wallet vs non-custodial wallet 11

2.2.5.3 Types: desktop, mobile, hardware, paper, online 11

2.2.5.4 Seed 12

2.2.5.5 Transactions and fees 12

2.3 Bitcoin 13

2.3.1 What is Bitcoin 13

2.3.2 Bitcoin history 14

2.3.3 What are altcoins? 14

2.4 Ethereum 14

2.4.1 Why is it important to know the basics of Ethereum and the Ethereum landscape? 14

2.4.2 What is Ethereum? 15

2.4.3 What is Ether? 15

2.4.4 What is ERC-20? 15

2.4.5 How do Ethereum smart contracts work? 15

2.5 Regulation of cryptocurrencies 15

2.5.1 FATF travel rule 15

2.5.2 AMLD5 and implementations in national laws 16
2.5.3 EU Digital Finance Package: Legislative proposals on crypto-assets, seizing opportunities and mitigating risks 16
2.5.4 MiCA guide 17
2.6 Criminal use of cryptocurrency includes but is not limited to 18
2.6.1 Darknet markets 18
2.6.2 Ransomware 19
2.6.3 Extortion 19
2.6.4 Scams 19
2.6.5 Ponzi-schemes 19
3 Practical guidelines on seizing 19
3.1 What is seizing/confiscation? 20
3.1.1 Crypto-assets vs normal assets 20
3.2 Pre-seizure planning 20
3.2.1 Introduction and legal framework 20
3.2.2 Training and expertise 21
3.2.3 Searching for? 22
3.2.4 Government-controlled wallets 23
3.2.5 Warrants, who has the power to decide? 24
3.2.6 Be aware of accomplices 24
3.2.7 Strategy and plan of action 25
3.3 Desktop Wallet 26
3.3.1 Introduction 26
3.3.2 Bitcoin Core and difference from “light wallets” 26
3.3.3 Electrum 29
3.3.4 Exodus 45
3.3.5 Ethereum Wallets 49
3.3.5.1 MyCrypto Wallet 49
3.3.5.2 Metamask 53
3.4 Mobile Wallet 65
3.4.1 Introduction 65
3.4.2 Best practices and guidelines 65
3.4.3 MyCelium 66
3.4.4 Jaxx Liberty 69
3.5 Hardware Wallet 74
3.5.1 Introduction 74
3.5.2 Best practices and guidelines 75
3.5.2.1 Ledger wallet 75

3.6 Paper Wallet 101
3.6.1 Introduction 101
3.6.2 Encrypted versus Non-Encrypted 105
3.7 Custodial and online web wallets 111
3.7.1 Introduction 111
3.7.2 Best practices and guidelines 114
3.7.3 Two-factor authentication (2FA) 116
3.8 Seeds 116
3.9 Reporting 117
4 Closing words 118

1 Introduction

Due to the Covid-19 pandemic, many businesses and institutions changed their activities from physical presence to an online environment, thus relying even more on technology. As criminals are adaptable by nature to the ongoing changes in a society, they also shifted their activities to the online world and preyed on the increasing number of internet users worldwide.

While performing criminal activities ranging from tax evasion to money laundering and drugs trafficking, perpetrators use more and more often cryptocurrency due to the privacy and anonymity it allegedly provides.

According to Europol's Internet Organized Crime Threat Assessment (IOCTA 2019), "*cryptocurrencies continue to facilitate cybercrime, hackers and fraudsters now routinely target crypto-assets and enterprises*", therefore, "*law enforcement and the judiciary must continue to develop, share and propagate knowledge on how to recognize, track, trace, seize and recover cryptocurrency assets*".

Despite the fact that cryptocurrencies are no longer a novelty, the use of eluding technology to hide the identity of users, the cross-border nature of transactions, the sometimes-inconsistent regulations while addressing financial transactions and inconsistencies in national legislation when dealing with illicit activities make it the currency of choice for many criminals.

Although guidelines on freezing and confiscation of virtual currencies sometimes exist on a national level, a guide with best practices and solutions on different challenges with an international perspective could prove beneficial to many state actors in countries across the world.

The *Guide on seizing cryptocurrency* was developed under the iPROCEEDS-2 project, result 4, "*Capacities of specialized investigative units and inter-agency cooperation between cybercrime, financial investigators, prosecutors, representatives of FIUs and cybersecurity experts in the search, seizure and confiscation of online crime proceeds, combating cybercrime and securing electronic evidence further strengthened*."

1.1 Rationale

Within the first year of implementation of the iPROCEEDS-2 project, the topic of virtual currency appeared on multiple occasions as the need for capacity building on this topic exists. Guidelines for freezing and confiscation of crypto currencies were requested by several iPROCEEDS-2 project countries/area along with support on drafting legislation on the matter.

1.2 The purpose of the Guide

Drafted by international experts on the matter, the Guide provides a set of general rules and best practices in relation to freezing and seizing of cryptocurrency.

The initiative transcends national approaches and provides an international insight into the topic that will be useful to many countries worldwide, when targeting crimes involving virtual currencies.

The expected outcome of developing such a Guide is an *enhancing of the capabilities of all state agencies* that target crimes that involve a financial aspect but not be limited to these.

1.3 To whom is the Guide addressed?

The Guide aims to come to the support of law enforcement, prosecutors, judges, Financial Intelligence Units, Financial Investigation Units, digital forensics experts and/or training institutions.

From the outset, the Guide was meant to provide step-by-step instructions to local authorities when dealing with virtual currency and to be a toolbox for all investigators on different occasions (house searches, arrests, etc.) when they expect to come across this type of asset.

2 Theory behind seizing

2.1 Definitions (FATF/EU)

Since the appearance of Bitcoin, there are various definitions in existence for virtual currency and blockchain technology. This subject was studied by numerous policymakers at the European Union level and the international level, such the International Monetary Fund, the Bank for International Settlement, and the Financial Action Task Force. Each of these policymakers touched on the subject in a different way, but apart from the Financial Action Task Force's statement of meanings, there are no internationally adopted definitions of these terms.

Considering the variety of different national regulations, the fact that this guide will have an international scope thus transcending national approaches, the Financial Action Task Force's and the bodies of the European Union's definition will be used for defining the terms.

2.1.1 Definition of "Virtual Currency", "Cryptocurrency" and "Virtual Assets

I. Financial Action Task Force

The Financial Action Task Force (FATF) published its virtual currency report in June 2014[1].

The report has distinguished virtual currency from fiat currency. Fiat currency is the most used monetary aggregate (or type of money), defined as coin and paper money of a country that is designated as its legal tender and accepted as a medium of exchange in the issuing country.

The report also differentiates virtual currency from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status.

Virtual currency is

- a digital representation of a medium of exchange
- and/or a unit of account
- and/or a store of value
- but does not have legal tender status
- it is not issued nor guaranteed by any jurisdiction
- and does not fulfil the above functions only by agreement within the community of users of the virtual currency

[1] http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Cryptocurrency is

- as a math-based
- decentralized convertible virtual currency
- that is protected by cryptography
- relies on public and private keys to transfer value from one person (individual or entity) to another
- and must be cryptographically signed each time it is transferred

The report states that hundreds (nowadays: tens of thousands) of cryptocurrency specifications have been defined, mostly derived from Bitcoin.

The FATF Recommendations has incorporated the definition of virtual asset in 2015[2].

Virtual asset is

- a digital representation of value
- that can be digitally traded, or transferred, and can be used for payment or investment purposes.

The FATF Recommendations underline that virtual assets do not include digital representations of fiat currencies, securities, and other financial assets.

II. EU institutions

The definitions by the EU institutions for the most part resemble the FATF definitions, except some small differences.

The Court of Justice of the European Union gave a preliminary decision on 22 October 20153, stating that Bitcoin is not used as asset, but as a special payment. Therefore, units of the bitcoin virtual currency are exempt from VAT under the provision concerning transactions relating to "currency, bank notes and coins used as legal tender".

The European Central Bank (ECB) does not regard virtual currencies as a full form of 'money', as defined in its analysis from February, 20154. The ECB declared that virtual currencies do not fit the economic or legal definition of 'money' or 'currency' and noted that they have a low level of acceptance among the public.

Based on the ECB's paper,

Virtual currency is

- a digital representation of value,
- not issued by a central bank, credit institution or e-money institution,
- in some circumstances, used as an alternative to money.

[2] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf
[3]Case C-264/14, http://curia.europa.eu/juris/liste.jsf?num=C-264/14
[4]https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

The European Banking Authority's (EBA) report on crypto-assets from January, 20195 provides a slightly different definition, creating the category of 'crypto-asset'.

Based on the EBA's report,

Crypto asset means an asset that:

1. depends primarily on cryptography and distributed ledger technology (DLT) or a similar technology as part of its perceived or inherent value;
2. neither is issued nor guaranteed by a central bank or public authority, and
3. can be used as a means of exchange and/or for investment purposes and/or to access a good or service.

The EBA's definitions include virtual currencies and tokens under the term 'crypto-asset'.

The European Parliament's study, named 'Cryptocurrencies and blockchain'[6], defined virtual currencies as cryptocurrencies.

According to the European Parliament's study,

Cryptocurrencies are

1. a digital representation of value
2. decentralized, i.e., not issued, nor guaranteed by a central bank or a public authority
3. not attached to a legally established currency
4. not possessing the legal status of currency or money
5. electronically transferable, storable, and tradeable

In the fifth Anti-Money Laundering Directive (Recital 10)[7] the European Commission extended the scope of the directive to virtual currency platforms and wallet providers and established the definition of virtual currencies.

Based on the fifth AML Directive,

Virtual currencies

- are a digital representation of value
- that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money
- but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored, and traded electronically

The fifth AML directive also underlines that virtual currencies should not be confused with electronic money within the scope of the EU Electronic Money Directive (2009/110/EU) or larger concept of funds within the scope as defined in the Second EU Payment Services Directive (2015/2366/EU).

[5] https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1
[6] https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

Summary

The definitions above imply that **virtual currency:**

- is distinguished from fiat currency (i.e., real currency, real money, or national currency)
- is distinct from e-money
- and is a subcategory of digital currency

Even though FATF made a differentiation between virtual currency and cryptocurrency terms, based on the EU definitions, 'virtual currency' interchangeably with the term of 'cryptocurrency'.

However, regarding the term of 'crypto asset', the EU bodies rely on the definitions of FATF. The existing proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets[8] refers to EBA's study, but also states that any definition of 'crypto-assets' should correspond to the definition of 'virtual assets' set out in the recommendations of the FATF, and any list of crypto-asset services should also encompass virtual asset services that are likely to raise money-laundering concerns and that are identified as such by the FATF.

2.1.2 Categorization of virtual currencies

The term 'virtual currency' has been mentioned by a CNN article in 2009, and it was used for hi5 coins and for game tokens, like Second Life's Linden Dollars or World of Warcraft's gold.[9] Although Bitcoin network came into existence in January 2009, the article did not mention it.

Various studies have categorized the virtual currencies, e.g., the European Central Bank's statement from 201210 or the IMF Discussion Note from 2016,11 but the FATF's categorization has been adopted internationally.

The mentioned FATF report on virtual currencies distinguishes:

- Convertible virtual currencies,
- Non-convertible virtual currencies,
- Centralized virtual currencies,
- Decentralized virtual currencies.

Convertible (or open) virtual currency, if

- it has an equivalent value in real currency and,
- it can be exchanged back-and-forth for real currency.

The study underlines that some convertible virtual currencies can be exchanged directly through the issuing administrator, others must be exchanged through a virtual currency exchanger. Bitcoin, Litecoin, Ether, Second Life Linden Dollars are convertible virtual currencies.

Non-convertible (or closed) virtual currency

- is intended to be specific to a particular virtual domain or world,
- because it only has a value in this virtual environment,

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593
[9] http://edition.cnn.com/2009/TECH/05/18/online.currency/index.html?eref=rss_tech
[10] https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
[11] https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

- cannot be exchanged for fiat currency outside the specific virtual domain or world.

This special virtual world can be a Massively Multiplayer Online Role-Playing Game (MMORPG), or an online shopping site (for example: Amazon.com for Amazon Coins).

It is worth to mention that an unofficial, secondary market may provide an opportunity to exchange the 'non-convertible virtual currency' for fiat currency or another asset, but the related companies have common practice and written prohibitive measures against these secondary markets.

Centralized virtual currencies

- have an administrator,
- that controls the system.

This administrator issues the currency, establishes the rules for its use, maintains a central payment ledger and has authority to withdraw the currency from circulation.

Second Life Linden dollar, World of Warcraft gold and the infamous OneCoin are centralized virtual currencies.

Decentralized virtual currencies are

- distributed
- open source
- math-based peer-to-peer virtual currencies
- without central administrating authority

Bitcoin, Ether and Litecoin are examples of decentralized virtual currencies.

It is worth pointing out that to in order to attract customers, the operators of some fraud systems – e.g., Ponzi schemes – promote their coins as decentralized virtual currencies, while their system is a centralized one.

2.1.3 Definition of "VASP"

The FATF Recommendations have incorporated the definition of virtual asset service provider in 201512.

Based on the recommendations, virtual asset service provider means any natural or legal person who as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- exchange between virtual assets and fiat currencies
- exchange between one or more forms of virtual assets
- transfer of virtual assets
- safekeeping and/or administration of virtual assets or instruments
- enabling control over virtual assets
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset

[12] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

As mentioned in Chapter 1.1.2., the EU institutions are using the term of 'crypto-asset' instead of 'virtual asset'.

The existing proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets (MiCA), created a new definition for crypto-asset and a new categorization for crypto-asset service providers, but it is based on the referred FATF Recommendations' definitions.

2.1.4 Definition of Distributed Ledger

Distributed Ledger Technology (DLT) is a well-known and commonly used technology. However, the international institutions like the European Commission's Joint Research Centre (JRC), the European Central Bank (ECB) have a different definition on the term.

Based on the JRC's study from 2019, DLTs are particular types of databases, in which the data is recorded, shared and synchronized across a distributed network of computers or participants[13].

Based on the ECB's research paper[14] a distributed ledger is a record of information, or database, that is shared across a network, and the best-known type of distributed ledger is "blockchain". Based on the research, the name comes from the fact that some Distributed Ledger Technology solutions store all individual transactions in groups, or blocks, which are attached to each other in chronological order to create a chain. This long chain is put together using a complex algorithm which ensures the security and integrity of the data.

The ECB's paper underlines the fact that access to a distributed ledger can be unrestricted, i.e., any party could become a participant, or restricted to a specified group of users. It means the members of the network may have access either to the entire ledger or only to part of it. Depending on the permission rights, members can add data, which are then disseminated to other members of the network. Allowing only authorized entities to make updates, could be a useful way to protect the network from malevolent users or external attackers trying to disrupt its functioning.

2.1.5 What is blockchain?

Referring to the JRC's study, blockchain is part of the broader meaning of DLTs. Blockchain technology is using cryptographic techniques to record and synchronize data in chains of blocks. The difference concerns the way data is distributed, verified, and registered. All types of blockchain are DLTs but not all DLTs are blockchains.

Based on the Global Blockchain Benchmarking Study from 2017, blockchain is a type of database that is replicated over a peer-to-peer (P2P) network. Blockchain is special, because it is a new type of database that enables multiple parties to share the database and to be able to modify it in a safe and secure way, even if they do not trust each other[15].

The Bitcoin blockchain is a public record of Bitcoin transactions in chronological order. This blockchain is then shared between all Bitcoin users. It is used to verify the Bitcoin transactions and to prevent double spending.

It can be consulted at many different websites, for example https://explorer.bitcoin.com/btc

[13] https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-now-and-tomorrow
[14] https://www.ecb.europa.eu/pub/annual/special-features/2016/html/index.en.html
[15] Global Blockchain Benchmarking Study by Dr Garrick Hileman & Michel Rauchs 2017, p. 13.

2.2 General concepts

2.2.1 What is Proof of Work?

According to the Bitcoin Wiki, a proof of work is a piece of data which is difficult (costly, time-consuming) to produce (by miners) but easy for others to verify and which satisfies certain requirements.

The goal for a miner is to find an arbitrary number (called a nonce, number only used once) that, when hashed with SHA-256, it corresponds with a predefined pattern (a number of leading zeros).

If a miner found a match, he sends his block to the Bitcoin network so every node could check its work if indeed the hashing follows the pattern. Finding the block is difficult, verifying it is relatively easy.

For example:

Needed pattern: 9 leading zeros

Used nonce by the miner: 2831785

Resulting hash after cryptographic function: 000000000a0e06c78b106b48d30b55bd2e5076aa13619072161145855b2eb93c

URL: https://live.blockcypher.com/btc/block/000000000a0e06c78b106b48d30b55bd2e5076aa13619072161145855b2eb93c/

When the Bitcoin network accepts the miners block, this miner will be rewarded with newly generated bitcoins. So mining is the process of hashing the block header repeatedly, changing one parameter, until there is a match with the desired output.

Since the hash of the previous block is also used in the cryptographical function, every block is linked to the previous one. In Bitcoin about every 10 minutes a new block is mined and each of these blocks contain Bitcoin transactions of that timeframe, selected from the memory pool of transactions and often driven by an incentive called the fee, which is then also rewarded to the miner.

The pattern changes every 14 days (or 2016 blocks). The number of leading zeros depends on the hashing power that exists in the network.

2.2.2 What is Proof of Stake?

In this consensus mechanism the users are required to stake an amount of their coins or tokens in order to have a chance of being selected by the network to validate a block of transactions. Just like in proof of work, this system also has an incentive, as the selected staking address received new coins or tokens.

The more tokens a user stakes in his wallet, the more chance there is of being selected and receiving new tokens.

Proof of Stake is considered as a much more environmentally friendly alternative to Proof of Work.

2.2.3 What is Yield Farming (in Decentralized Finance)?

Yield farming is a popular practice on the Ethereum network and is somewhat like staking. Yield farmers stake or lock their tokens in a decentralized finance application (DeFi). In return they get the native token of that DeFi app plus a share of the transaction fees. It all depends on the type of DeFi app how the yield farmer will be rewarded.

2.2.4 What is a public-private key pair?

Major cryptocurrencies like Bitcoin are built upon asymmetric cryptography that uses public/private key pairs: public keys are publicly known, and private keys are kept secret.

For Bitcoin, the public key is derived from the private key through a one-way cryptographic function (known as elliptic curve multiplication). The bitcoin address is generated from the public key through a one-way cryptographic hash function (see below).

A private key is a simply randomly generated number. Control over a private key gives access to all funds associated with the corresponding address. To spend bitcoins, a private key will be required.

But often on top of the private key(s) a password or PIN will be needed for a seizure (see below).

2.2.5 What is a wallet?

2.2.5.1 Definition

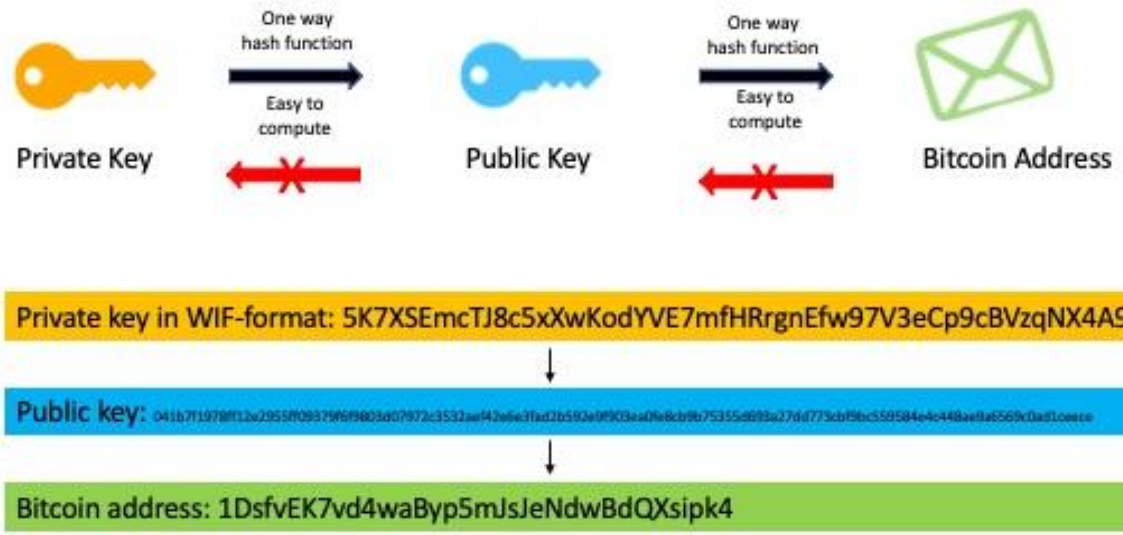
A cryptocurrency wallet can be either a physical hardware device, a program or a service which stores public and private keys. It can be considered as a user interface that controls access to a user's money.

Nowadays, most wallets are hierarchical deterministic wallets (or HD wallets), where all the keys are derived in a tree-like structure from a single master key, known as the seed.

The screenshot above shows the HD icon. It is taken from the Bitcoin Core wallet (v0.20.1). In the early days of Bitcoin, starting from 2009, this was the only wallet available, but it was not HD back then (and was called Bitcoin-Qt). Users had to backup this wallet very often. HD wallets do not need this kind of maintenance.

There is sometimes a misunderstanding that crypto wallets contain cryptocurrencies. They only contain the private keys which allow the user to spend the cryptocurrencies with the associated public key.

For example: A private key in Bitcoin Core is cryptographically linked to a public key. In its turn, this public key is, cryptographically linked to a particular bitcoin address. The private key can control the bitcoins at its bitcoin address.



2.2.5.2 Custodial wallet vs non-custodial wallet

In a custodial wallet, the private keys are held by a third party. This can be a financial institution or a cryptocurrency exchange platform. A non-custodial wallet, also known as a self-hosted or self-custody crypto wallet is a type of wallet that let individuals store and use their private keys/cryptocurrencies. Examples of a non-custodial wallet are Electrum, Ledger wallet and Jaxx Liberty.

2.2.5.3 Types: desktop, mobile, hardware, paper, online

Depending on your cryptocurrency use, you might have or use multiple different type of wallets.

Desktop wallets are often used as local storage on a computer, by people that might not necessarily use them on a daily basis.

These are often online (hot) wallets which are considered a bit more unsecure due to different types of malware that are specifically designed to compromise these wallets.

An example of that type of malware is called Coinbitclip. This malware is designed to replace the public key when a user is sending bitcoins. The trojan uses a very similar looking Bitcoin address with the result that the bitcoins are sent to the bitcoin address of the malware.

These desktop wallets can also be used as a shared wallet. For example, you can use your desktop wallet on your mobile phone app by setting it up with the same seed word.

Exodus wallet is a good example of a wallet that can be used on the desktop and on a mobile device. During the installation process you just restore the wallet with the same seed words on the other device or you have the option to scan the QR code with a mobile device and both wallets will be synced.

Mobile device wallets are used more on a daily basis use case. When you go to a cryptocurrency kiosk (ATM) you show the QR code from the mobile device to the kiosk to deposit cryptocurrency to the desired address. Vice versa, if you want to sell cryptocurrency from the wallet you scan the QR code given by the kiosk to send the specific amount you want to sell to the given address by the kiosk.

Paper wallets were often the first type of wallets Bitcoin users started to use. These wallets were typically printed on paper or kept in a PDF file digitally. In a normal paper wallet, you have a public and a private key. The problem with a paper wallet is when the private key is destroyed, either partially or fully, one loses all access to the cryptocurrencies and hence it is not a very safe way to keep these assets on.

Paper wallets are still found from time to time in suspects' homes, either with a QR code and the associated public – private keypair or just in simple text format. These are very important to recognize in both formats. Setting up a paper wallet is addressed later in this manual.

Hardware wallets have lately become the industry standard for individual use. They provide hardware level encryption and a very safe method to store many different cryptocurrencies. Setting up a Ledger hardware wallet is addressed later in this manual. When using a hardware wallet such a Ledger or Trezor, the most important thing is to safekeep the seed words. Misplacing these compromises your wallet.

Lastly, there also exist online or so-called web wallets. These crypto wallets can be run in a web browser. However, there is a big security concern here since these wallets are susceptible to cyber-attacks or thefts (e.g., the Coinbitclip trojan). Examples of web wallets are block.io and blockchain.com.

2.2.5.4 Seed

Today's wallets are practically all hierarchical deterministic wallets (or HD wallets), defined by the Bitcoin Improvement Proposals BIP0032 and BIP0044.

These HD wallets make use of a seed that is created from a list of English words that form a mnemonic. A mnemonic is a series of 12 to 36 words that store all the information needed for the recovery of a cryptocurrency wallet.

When first creating a HD wallet, the user will be shown 12 or in some cases 24 English words that will create this seed.

A single backup (of the mnemonic) at creation time of the wallet is sufficient since the seed (via the mnemonic) can re-create all private keys of the wallet.

The English words and the mnemonic are part of the BIP0039 standard. The full list is available at following URL: https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt

An example of a mnemonic is the following word sequence. It was created on the website https://iancoleman.io/bip39/#english:

> *hurt toss large spider review donate execute coconut torch place small foil*

A list of all Bitcoin Improvement Proposals (BIP) can be seen at https://github.com/bitcoin/bips.

2.2.5.5 Transactions and fees

A transaction is a transfer of value between participants (or wallets) in the cryptocurrency ecosystem which will be recorded in a blockchain. For instance, a transfer of 1 bitcoin from bitcoin address A (sender) to bitcoin address B (recipient). A transaction fee can be considered as a financial incentive for the miners.

Explaining the ins and outs (literally) of transactions, however, is not the purpose of this guide. Just remember that a transaction exists of:

1. A transaction ID (hash value)
2. The number of bitcoins that were sent
3. A transaction fee
4. One or more transaction inputs (aka UTXO's)[16] or address(es) of the sender
5. One or more transaction outputs (one or more receiver addresses and possibly one or more change addresses

See below an example from blockchain.com[17] with two inputs and two outputs, one output is considered the payment and the other is considered to be the change:

2.3 Bitcoin

2.3.1 What is Bitcoin

Bitcoin is an asset, a protocol and a peer-to-peer network created in 2009 by Satoshi Nakamoto, an alias for the unknown inventor or inventors of Bitcoin that can be used for instant payments. Satoshi Nakamoto reached a breakthrough in 2008 for using computer code to authenticate and secure transactions without resorting to a centralized bank or government treasury.

The Bitcoin whitepaper was published on 31 October 2008 and can be downloaded at: https://bitcoin.org/bitcoin.pdf.

Transactions in the Bitcoin network are made without middlemen like banks or governments. Or as Nakamoto summed it up: "a purely peer-to-peer version of electronic cash" that allows "online payments to be sent directly from one party to another without going through a financial institution."

The balance of each bitcoin address is kept on the Bitcoin blockchain, a public ledger that everyone has access to.

The Bitcoin protocol uses various encryption techniques to regulate the generation of units of currency and verify the transfer of funds.

Bitcoin is open source and thus its code is part of the public domain. Nobody owns or controls Bitcoin and thanks to the peer-to-peer technology, everyone can participate.

"Bitcoin" - with capitalization, is used when describing the concept of Bitcoin, or the entire network. "bitcoin" - without capitalization, is used to describe bitcoins as a unit of account.

[16] UTXO: *Unspent Transaction Output. More info at: https://en.wikipedia.org/wiki/Unspent_transaction_output*
[17] https://www.blockchain.com/btc/tx/3f8a389b807382e2ab85590a77df7de0de8de9bce05fdffcdc40df99cbfc5092

2.3.2 Bitcoin history

Bitcoin uses concepts and technologies that existed before its conception. For example, the ideas behind proof-of-work, and a blockchain (ledger) already existed. The use of timestamps and computational puzzles were not new either. Bitcoins' creator, Satoshi Nakamoto, called upon these already existing technologies. He added the distributed ledger concept as an important finishing touch. It made Bitcoin what it is now.

2.3.3 What are altcoins?

Altcoins or *alternative coins* are all other cryptocurrencies that are not Bitcoin. There exist thousands of altcoins on the cryptocurrency market which can be viewed on websites like https://coinmarketcap.com/

Examples of altcoins are: Ethereum, Litecoin, Monero, and so on.

2.4 Ethereum

2.4.1 Why is it important to know the basics of Ethereum and the Ethereum landscape?

Ethereum was first introduced in 2013 and the Ethereum blockchain went live in 2015. Compared to Bitcoin it is not only a cryptocurrency. The Ethereum platform is a decentralized blockchain that was made to store code and computer programs that can be executed anywhere and just like in Bitcoin, it cannot be shut down due to the decentralized nature.

Ethereum has a decentralized replicated virtual machine, called the Ethereum Virtual Machine (EVM), which can execute Turing-complete scripts and run decentralized applications.

Ethereum is the second most popular cryptocurrency in market size according to Coinmarketcap.com. One can run an Ethereum archive node which would store all the data ever been published into different projects and code but that would take around 4 to 5 terabytes of storage space. Ethereum blockchain itself is still under 200 gigabytes, but those are only the transactions that have been stored directly to the blockchain.

Smart contracts

Smart contracts are self-executing contracts in which the terms and conditions between two parties are written in the code itself. The use of the Ethereum blockchain with a smart contract could be described like the following example: image that you want to buy a car and the payment plan is stored on an Ethereum contract. Once you have made the last payment, the contract self-executes the final step which is sending you the paperwork of your car to close the contract.

Initial Coin Offering (ICO)

Also, a few years ago the Ethereum network was started to be used as an initial coin offering platform which is the digital equivalent to an initial public offering (IPO). In just a few months many different projects created their own native tokens (ERC-20 type tokens) in which anyone could buy in with Ether or even bitcoin.

Accounts and transactions

The main difference between Ethereum and Bitcoin is that for an Ethereum transaction, which initiates a "state change" of the account, one only needs to send the exact amount of Ether which then creates

or initiates this state change. No excess change (change address) is created like in Bitcoin, since only the needed amount will be sent. It also saves transaction kilobits compared to Bitcoin transactions. After a transaction, the value is deducted from you Ether account (accounts, which also use public-private keys).

2.4.2 What is Ethereum?

Simply put, Ethereum is an open source blockchain platform where Ether (ETH) and many different Ethereum tokens are used either as a means of payment or implemented in a smart contract.

2.4.3 What is Ether?

Ether is the native cryptocurrency of Ethereum. It stores value like in Bitcoin, but its transfers are more "economical" in that sense that only the state of your Ether wallet changes.

2.4.4 What is ERC-20?

ERC-20 is an Ethereum standard for smart contracts on the Ethereum blockchain where all ERC-20 tokens reside. A complete list of all ERC-20 tokens can be found at https://etherscan.io/tokens.

In order to send these tokens, a small amount of ETH in the wallet is necessary.

2.4.5 How do Ethereum smart contracts work?

As explained above, a smart contract is a trustless program that self-executes a predetermined action when certain conditions are met. This "action" will be an Ethereum transaction that for instance, releases a monthly payment to one or more employees or updates a step in the supply chain of a company.

2.5 Regulation of cryptocurrencies

2.5.1 FATF travel rule

In 2019, the FATF adopted an Interpretive Note to Recommendation 15 to further clarify how the FATF requirements should apply in relation to Virtual Assets and Virtual Asset Service Providers. In June 2020, the FATF adopted the 12-month review of the revised FATF standards on virtual assets and virtual asset service providers (VASPs)[18].

In these documents, FATF states that to manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

With respect to preventive measures, VASPs are subject to the following qualifications:

- The occasional transactions designated threshold above which VASPs are required to conduct customer due diligence is USD/EUR 1 000

[18] http://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

- Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers and make it available on request to appropriate authorities

2.5.2 AMLD5 and implementations in national laws

In the fifth Anti-Money Laundering directive, (5th AMLD) the European Commission extended the scope of the directive to virtual currency platforms and wallet providers, and it states that virtual currencies should not be confused with electronic money within the scope of the EU Electronic Money Directive (2009/110/EU) or larger concept of funds within the scope of the revised Second EU Payment Services Directive (2015/2366/EU).

The Commission proposes a framework on crypto-assets to allow for innovation but with preserving the financial stability and protecting the investors, because crypto-assets can serve as an access key to a service, could facilitate payments, or could be designed as financial instruments.[19]

The Commission differentiates between those crypto-assets already governed by EU legislation, and other crypto-assets, which step will enable market participants and regulators to gain experience with the use of DLTs exchanges. The Commission proposes a pilot regime for market infrastructures that wish to try to trade and settle transactions in financial instruments in crypto-asset form.

2.5.3 EU Digital Finance Package: Legislative proposals on crypto-assets, seizing opportunities and mitigating risks

The Digital Finance Package

On the 24th of September 2020, the European Commission adopted the Digital Finance Package. The objective of the proposal is to lay the foundations of a new strategy on digital finance for the EU financial sector, and its main goal is to ensure that the EU embraces the digital revolution and drives it with innovative European firms in the lead, making the benefits of digital finance available to European consumers and businesses. By making digital-friendly rules and granted safe for consumers, the Commission aims to leverage synergies between high innovative start-ups and established firms in the financial sector while addressing associated risks.

It is worth to mention that this proposal is the first, entirely virtual currency related regulatory proposal in the European Union.

Legislative proposals on crypto assets

The Commission proposes a framework on crypto-assets to allow for innovation but with preserving the financial stability and protecting the investors, because crypto-assets can serve as an access key to a service, could facilitate payments, or could be designed as financial instruments.[20]

The Commission differentiates between those crypto-assets already governed by EU legislation, and other crypto-assets, which step will enable market participants and regulators to gain experience with the use of DLTs exchanges. The Commission proposes a pilot regime for market infrastructures that wish to try to trade and settle transactions in financial instruments in crypto-asset form.

[19] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

[20] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

The Commission proposes a framework on crypto-assets to allow for innovation but with preserving the financial stability and protecting the investors, because crypto-assets can serve as an access key to a service, could facilitate payments, or could be designed as financial instruments[21].

The Commission differentiates between those crypto-assets already governed by EU legislation, and other crypto-assets, which step will enable market participants and regulators to gain experience with the use of DLTs exchanges. The Commission proposes a pilot regime for market infrastructures that wish to try to trade and settle transactions in financial instruments in crypto-asset form.

2.5.4 MiCA guide

As part of the Digital Finance Package, the Commission published its proposal on Markets in Crypto-Assets (MiCA). The proposal focuses on the issuance of **crypto-assets** and the provision **of crypto-asset service providers.**[22]

The goals of MiCA are to establish uniform requirements, to ensure a wider scope of application to the crypto-asset industry.

These requirements are:

- transparency and disclosure
- authorization and supervision
- operation, organization, and governance
- consumer protection
- prevention of market abuse

Based on the proposal,

Crypto asset is

- a digital representation of value or rights
- which may be transferred and stored electronically
- and use distributed ledger, or similar technology

The proposal underlines that these instruments are **not crypto assets**

- MiFID II financial instruments
- EMD2 electronic money
- deposits
- structured deposits
- securitization

The proposal differentiates **stable coins**, creating two new categories

- asset-referenced tokens
- electronic money tokens

[21] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

Numerous provisions apply to all crypto assets. More strict requirements apply to stable coins which are categorized as either asset-referenced tokens or e-money tokens. The most stringent requirements are for stable coins that are designated by the European Banking Authority as significant.

The proposal also stated that **issuers of crypto assets**

- are required to be incorporated as a legal entity
- to produce and publish a whitepaper ahead of any issuance
- and to adopt standards on marketing

MiCA also noted that whitepapers must contain prescribed minimum information but do not need to be approved in advance by any institution unless they relate to asset-referenced tokens or e-money tokens. However, issuers of asset-referenced tokens and e-money tokens will need to be authorized by a regulator.

Based on the proposal, the enlisted services would be regulated under MiCA, as service provider.

Crypto-asset service providers in the definition responsible for

- the custody and administration of crypto assets
- the operation of a trading platform for crypto assets
- the exchange of crypto assets for fiat currency
- the exchange of crypto-assets for other crypto-assets
- the execution of orders for crypto assets on behalf of third parties
- the placement of crypto assets
- the reception and transmission of orders for crypto-assets; and advice on crypto-assets

MiCA defined sets of activities for which crypto-asset service providers must be established as legal entities and must be authorized, these companies have to comply with regulatory provisions such as conduct customer asset safeguarding, market abuse and prudential requirements.

2.6 Criminal use of cryptocurrency includes but is not limited to

2.6.1 Darknet markets

Darknet markets are where Bitcoin and other cryptocurrencies might have gotten their first real use. The notorious Silk Road started in the year 2011 and it marked the beginning of a totally new category of criminality. Some say that the founding of Silk Road gave actually the first value to Bitcoin and thereafter other cryptocurrencies. From darknet markets you can buy anything imaginable (mostly illicit goods and services such as drugs, real/fake passports and driver's licenses, counterfeit money, credit card information, …). To access these markets, you typically need to install special anonymization software like Tor or I2P which makes the user anonymous and invisible through encryption. Darknet markets typically have had a plague on exit scams in which the owner of the market runs off with all the funds that are sitting in the escrow accounts. Recent law enforcement actions have taken many of these markets down with the administrators arrested and charged and often the cryptocurrencies seized.

Despite these actions, there is still a (growing) number of darknet markets that can be found on the Dark Web. Most of these markets accept Bitcoin. Some more privacy/security focused markets accept only Monero.

2.6.2 Ransomware

The year 2020 has been called the year of ransomware. It was estimated that payments of ransomware went up by more than 50% and campaigns have been more targeted. Ransomware encrypts the victim's computer or network and asks a ransom in bitcoins. These ransom demands can be anything between hundreds of dollars to millions. Garmin was hit by the ransomware called NetWalker in July 2020 and the demand was estimated to be 11 million US dollars. Some of these actors might be state actors and extorting victims in order to circumvent sanctions (DPRK). By paying these actors the company or individual might actually be in violation of sanctions set by the OFAC, who actively blacklisted different cryptocurrency addresses and actors.

2.6.3 Extortion

In the past few years, we have seen a lot of different cryptocurrency extortions due to the shared amount of data breaches available. The typical extortions are mainly the ones where a person receives an email stating the real name of the victim with a real password found in some breach. The email says that the extortionist has some compromised video material of the victim. It asks for a few hundred dollars in bitcoins in order to not publish this data to relatives, workplace or to a social media platform. There is no evidence that many of these are real, but in some cases, there has been noticed that some victims have been compromised through hacked Wi-Fi networks, where the victim has done something indecent in front of the webcam. These "real" cases have however happened very rare.

2.6.4 Scams

Scams are mainly crypto-related investment opportunities or "fake" initial coin offerings (ICOs) that are being advertised even by publicly know persons. In 2019 one of the largest scams, called PlusToken, was taken down with an estimated gain of 6 billion dollars. The PlusToken scam controlled more than 1.1% of all bitcoins in circulation. These scams are mostly targeting fintech investors or just common people that want to ride the FinTech wave and are fueled by greed. It has been seen that celebrities and even royalties' names have been used in fake campaigns to promote these investment opportunities.

2.6.5 Ponzi-schemes

The hype of Bitcoin has created new types of scams, the 'bitcoin-look-a-like' Ponzi schemes, such as OneCoin. OneCoin operated with a Multi-Level Marketing system. They advertised with pop-up windows, YouTube videos and Facebook groups, with the promise of unrealistic returns, such as 15-25% per month. In these marketing materials they compared OneCoin to Bitcoin and stated that they are using a new blockchain technology. In order to attract customers, OneCoin was promoted as a decentralized virtual currency, while the system in fact was centralized with a central administrating team, who issued the coin, established the rules for the network and had authority to withdraw the currency from circulation. OneCoin managed to net $4 billion and was named as 'one of the biggest scams in history' by the Times magazine.[23]

3 Practical guidelines on seizing

In general, with any virtual currency seizure or confiscation, we can identify the steps below:

- Pre-seizure planning
- Information collecting and/or tracing the trail of the virtual currency

[23] https://www.thetimes.co.uk/article/the-4bn-onecoin-scam-how-crypto-queen-dr-ruja-ignatova-duped-ordinary-people-out-of-billions-then-went-missing-trqpr52pq

- Taking control of virtual currencies
- Management and disposal of the secured virtual currencies

3.1 What is seizing/confiscation?

Seizure or confiscation is the act of taking the criminal related assets or evidence by legal process or force, such as the seizure of evidence found at the scene of a crime.

In the European Union, the 2014/42/EU Directive on the freezing and confiscation of instrumentalities and proceeds of crime in the EU widen the scope of the law enforcement authorities to trace, freeze, manage and confiscate the proceeds of crime. The Directive underlines that the Member States must take the necessary measures to enable the confiscation of instrumentalities and proceeds or property the value of which corresponds to such instrumentalities or proceeds, subject to a final conviction for a criminal offence, which may also result from proceedings in absentia.[24]

3.1.1 Crypto-assets vs normal assets

The main difference between crypto-assets and normal assets is that usually there is no centralized authority in the system – especially in decentralized virtual currencies – and the traditional monitoring of the transactions is not an option.

It does not mean that we cannot use the financial records of the suspect: large number of financial institutions (e.g., banks) listed the virtual currency related transactions, and sometimes this information can be a lead to identify the suspect's preferred crypto exchange.

However, the seizure, freezing or confiscation is quite different from the usual forms.

3.2 Pre-seizure planning

3.2.1 Introduction and legal framework

The cryptocurrency ecosystem is global and borderless with divergent national regulations. On the website https://bitnodes.io a visualization of the Bitcoin network can be found which shows how widespread this network is around the world.

When doing a seizure, first, it is important to know if there are applicable laws for seizing cryptocurrencies implemented in a specific country. Even though there are worldwide standards for seizing virtual currencies, the administrative practice and the existing case-law are different in each country, even in the Member States of the European Union.

Probably in some countries around the world there will be no laws nor legal frameworks regarding seizing of cryptocurrencies. In other countries existing laws of seizing assets (e.g., money) in criminal cases will be applicable on cryptocurrencies too.

To avoid any unlawful behavior (e.g., obtaining evidence in an illegal way) and procedural mistakes, it is important to understand the applicable legal framework and procedures for the seizure of cryptocurrencies.

Always keep in mind the relevance of seizing. The motivation of asset recovery could be diverse such as recovering proceeds for victims of scams and hacking or taking illegal proceeds from criminals obtained through various forms of crime. Take into consideration that the seizure of illegal proceeds

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0042

(depending on the amount and so) can be a much harder punishment for some criminals than an imprisonment. With this last comment it is our intention to emphasize the importance of seizing assets from criminals. In general, law enforcement and other relevant services should put even more efforts and time in taking illegal proceeds from criminals. To improve the success rate, good preparation will be essential.

Access to cryptocurrencies through (a) private key(s) or a seed phrase can be found locally e.g., on a desktop computer (i.e., a non-custodial wallet such as Electrum) or can be stored somewhere online on a custodial wallet in the same or another jurisdiction.

In fact, cryptocurrencies can be stored in various forms. Later, you will see that the seizing techniques for custodial wallets differs from non-custodial wallets.

Seizing funds from non-custodial wallets can be much more complicated as the funds will be controlled by a suspect and eventually by their accomplices. Because of this, it can be much harder to get control over the funds to seize them than in the case of custodial wallets. Of course, considering that the VASP (e.g., exchange) is cooperative with law enforcement.

Because of that, a good preparation and strategy will be relevant to increase a successful outcome of a seizing.

What follows is a non-exhaustive overview of topics to be considered and good practices at the stage of pre-seizure planning.

3.2.2 Training and expertise

Seizing cryptocurrency proceeds can be very challenging and requires a specific mindset. Due to its complex nature, it is advised that cryptocurrency seizures are carried out by competent law enforcement officers and if possible, by (specialized) law enforcement units experienced with cryptocurrency seizing.

The necessary competences can be acquired through training and practice. The more training and practice the better.

Several trainings have been developed that cover cryptocurrency seizing. An example of such a training was developed in 2019/2020 within the EMPACT framework. This "Cryptocurrency and Dark Web Investigations" on-site training package was developed by several law enforcement agencies and international organizations such as the Belgian, Austrian, Norwegian and Spanish police as well as EUROPOL, INTERPOL, SELEC, UNODC, ECTEG and OSCE. One of the lessons covered in this training is about cryptocurrency seizing (using Bitcoin Testnet etc.). This training package is property of ECTEG and can be requested from ECTEG by law enforcement agencies. Nowadays, many private companies that offer tracking and tracing solutions for cryptocurrencies, for example Chainalysis, also provide certified training packages starting from cryptocurrency fundamentals all the way to specialized investigation trainings.

Because of the increased use (both in criminal and non-criminal cases) and global acceptance of cryptocurrency, law enforcement officers that could be potentially confronted with cryptocurrency seizing should be able to recognize at least the most relevant traces regarding the use of cryptocurrencies. It is important to raise awareness of the more common concepts and use of these new technologies within law enforcement organizations. For example, law enforcement officers should be able to recognize QR codes, seed phrases, public and private keys, cryptocurrency address formats, wallets, etc.

For seizing purposes, recognition of the different address formats of cryptocurrencies is also important. When a law enforcement officer is unable to figure out which cryptocurrency is used, then seizing could become a problem to transfer these cryptocurrencies to the correct address format and corresponding government-controlled wallet. For example, Bitcoin needs to be transferred to a Bitcoin address (starting with 1, 3 or bc1) and Ethereum to an Ethereum address (starting with 0x).

When finding an unknown address format, there are tools (e.g., on the Internet) which can be helpful to find out which cryptocurrency is used. Some cryptocurrencies have a very limited use case and could be much harder to seize.

When performing a seizure, good knowledge about cryptocurrency wallets and different types of wallets (mobile, custodial, desktop, hardware, paper) is essential. Later in this guide, for each type of wallet will be covered in detail how a seizure could be executed. Some wallets support only one cryptocurrency (e.g., Bitcoin Core), other wallets support multiple cryptocurrencies (e.g., Exodus).

3.2.3 Searching for?

When confronted with a seizure of cryptocurrencies, several specific things could be relevant to search for such as

- Cryptocurrency addresses/public keys
- Private keys and seed word lists
- QR codes
- PINs
- Wallets
- Passwords
- Mining equipment
- Etc.

These cryptocurrency related things can be found, for instance in a building during a house search, on the body or in the pockets of a suspect during arrest. In many cases, it will be known in advance that chances are high that cryptocurrencies will be found, but sometimes the presence of cryptocurrencies will come unexpectedly. For example, one expected to find a cannabis plantation but instead a mining farm was found.

Be aware that most of the above-mentioned things are very easy to hide or to destroy.

As an example, think of the difference between one million Euro in cash and the equivalent of the same amount in bitcoins accessible through a private key or a 12-word seed on a simple note.

It is important to take this into account before kicking in a door or ringing at a doorbell. Depending on the case specific (preparatory) measures and/or tactics may be necessary (see below - plan of action).

If possible, it is a good practice to prepare the seizure in advance and trying to figure out which cryptocurrencies and wallets the suspect might be using. Sometimes, indications of which cryptocurrencies a suspect is using can be obtained beforehand through an already initiated investigation. E.g., a darknet vendor is selling counterfeit goods and needs to be paid with Bitcoin.

In general, the chance that Bitcoin is used in a criminal case is very likely. But lately an increased use of privacy coins is observed such as Monero and Zcash. For example, some darknet marketplaces only accept Monero such as White House Market.

Also, be aware that in many cases chances are high that access to cryptocurrency wallets will be protected by passwords or PINs. Even though the access to a wallet is open and unlocked, it is probable that a password or PIN is required to transfer funds. More particularly, in order to seize the cryptocurrencies and send them to a government-controlled wallet, probably a password or PIN will be required. Because of that, searching for passwords or PINs could become necessary. There are many places where passwords or PINs can be found such as under a keyboard, on a post-it, in an agenda, etc. Sometimes passwords can also be obtained through special investigative techniques such as memory analysis. Hardware and mobile wallets can be protected by a PIN.

In some countries depending on the legal framework, it just will be possible to ask the password from a suspect without one being able to speak of self-incriminating. In some jurisdictions, a suspect can even obtain sentence reduction if being cooperative with law enforcement.

The same applies for seed phrases. Very important to know is that with a seed phrase the requirement of a password (or PIN) can be bypassed (see below).

Hereafter you can find an overview of some relevant cryptocurrency related things to look for.

Name	**Bitcoin**	**Ethereum**	**Ripple**	**Litecoin**	**Dash**	**Monero**	**Zcash**
Ticker	BTC	ETH	XRP	LTC	DASH	XMR	ZEC
Address starts with	1, 3, bc1	0x	r	L	X	4	t1, t3, z1, z3
Address length	26-35	42 hex	34	34	34	95	35 or 96
Private key starts with	5, L, K	random	s, p	6, T	7, X	random	K, L
Private key length	51/52	64 hex	51/52	51/52	51/52	64 hex	51/52

3.2.4 Government-controlled wallets

A government-controlled wallet is a wallet under control of the government or state. More particularly, depending on the legal framework, this wallet can be under control of a law enforcement agency, a Court, an (investigative) judge, a public prosecutor, a confiscation body, a private company dealing with asset management, or even an auction house.

Depending on the legal framework and applicable seizing procedures of a country, the appearance of government-controlled wallets can take various forms. For example, it can be a hardware wallet, a paper wallet, a multi-signature wallet or the asset management can be under control of a third party such as a private company or auction house.

As mentioned before, when seizing cryptocurrencies, they need to be sent to a suitable address of an appropriate government-controlled wallet e.g., bitcoins need to be transferred to a Bitcoin address and Monero to a Monero address etc. Some wallets only support one cryptocurrency, others multiple cryptocurrencies (see above).

If applicable (i.e., taking into consideration the corresponding legal framework and seizing procedures), it is a good practice to prepare the proper seizing address(es) and government-controlled wallet(s) in advance as soon as there is a chance to be confronted with a cryptocurrency seizure.

Note: the seizing address is the address where the seized cryptocurrencies will be sent to.

Depending on which cryptocurrencies are to be found, there could be a necessity to prepare several government-controlled wallets such as one for Bitcoin, another one for Monero and so on or instead of these different wallets a multi-currency wallet can be used. This wallet preparation method can differ from country to country.

Thus, if applicable, the creation of these addresses/wallets must be done in a safe computer environment and strongly recommend having a written step-by-step guide as a projection of the internal rules.

It is advised to use a single address for every suspect seizure or confiscation.

Creation of a government-controlled wallet

In some countries the seizing address(es) will be provided by a confiscation authority or obtained through a web interface of a private company (responsible for asset management) or auction house. In these cases, there will be no need for law enforcement to create wallets for seizing purposes.

In other countries the creation of such wallets and secure asset management will be under control and responsibility of law enforcement.

3.2.5 Warrants, who has the power to decide?

According to the applicable legal framework, law enforcement officers responsible for a cryptocurrency seizure must be in possession of the right warrants. Also, in some jurisdictions it is important to know who has the power to decide on a seizure.

Relevant questions to ask are: which warrants/court orders are needed for a cryptocurrency seizure? Who has the power to decide for a cryptocurrency seizure? Etc.

It is also important to understand that a seizure of a computer (containing a software wallet), a hardware wallet device and a paper wallet for example is not sufficient. Also, copying a DAT file (containing a wallet) from a computer will not be sufficient. Seizing a computer, or a hardware wallet, … is not equal to seizing cryptocurrencies.

As reflected many times in this guide **a transaction/transfer to a government-controlled wallet will be necessary to effectively seize cryptocurrencies**. Besides a search and seizure order in some jurisdiction's additional warrants/court orders could be required. For example, a court order allowing to do a transfer for seizing purposes.

3.2.6 Be aware of accomplices

As mentioned, when seizing cryptocurrencies, speed of action can be crucial as there could exist one or more backups (e.g., private keys, seed phrases) of the suspect’s wallet(s) and accomplices could be

instructed to immediately transfer the funds to a wallet outside of control of government the moment they got triggered of a law enforcement action against the suspect.

Because of that, during a house search for example, it is important to separate the suspect (and his/her relatives) immediately from any device with which communications can be made such as a mobile phone and to control the suspect (and his/her relatives) in a way that no evidence can be disposed of nor any interactions with the outside world could be made possible (see below).

3.2.7 Strategy and plan of action

Several tips regarding strategies and plan of actions were already explained before.

Thus, when seizing cryptocurrencies, it is very important to understand what to look for and to have a good knowledge of the main concepts which are relevant for a seizure. This knowledge can be acquired through training and practice. Also, having a good understanding of the applicable legal framework and seizing procedures which can differ from country-to-country are essential. Next, regarding a cryptocurrency seizure, if applicable, know who has the power to decide and dispose of the right warrants/court orders for a seizure.

Another important step regarding pre-seizure planning is organizing good briefings in which can be explained what to look for and how the plan of action looks like.

Make sure you have prepared the appropriate equipment and have the right skilled (specialized) colleagues on-board.

Again, seizures take time and planning, do not wait with that just before kicking in a door.

A seizure can occur in different situations. In many cases, it will be possible to have a decent preparation but sometimes this will not be the case like when performing a house search in which is not expected to find cryptocurrencies.

Thus, wherever possible, it is advisable to determine an efficient strategy and plan of action for intervention. The manner of intervention will be essential to avoid that a suspect shall be able to make the wallet(s) inaccessible or destroy evidence. For example, the moment a suspect is alarmed of a police intervention at his premises, the suspect could switch off an encrypted computer, lock a smartphone and/or wallet mobile app or alert an accomplice who can already transfer the funds before law enforcement are able to.

In some cases, law enforcement can deploy a decoy to distract a suspect.

Ideally, the police intervention must be performed in such a way that a suspect has no options to do any manipulations.

When dealing with cryptocurrency seizing, time is essential. If possible, act immediately. The cryptocurrencies will effectively be seized once they are transferred to a government-controlled wallet.

Depending on which cryptocurrencies and type of wallets (e.g., custodial vs. non-custodial) are used, the seizing procedure could be different and require a different approach and plan of action.

Remarks

Sometimes the presence and use of cryptocurrencies will be detected afterwards, during the forensic analysis at the office of the suspect's devices. At that moment, if the cryptocurrencies are not transferred yet, it will still be possible to seize them.

Occasionally, it can also happen that it will not be possible to do a seizure on-site because of lack of equipment, specialized officers, warrants, etc. Keep this in mind and try to avoid these situations from taking place.

Depending on which government-controlled wallet and/or procedure will be used, an option could be to have prepared in advance the seizing address as a QR code to avoid typos. Right before executing a seizure, this seizing address needs to be double-checked to see if the address is still correct. A suggestion hereby is to use the four-eyes principle in which four eyes can check the correctness of the seizing address and hence safeguard the persons who are seizing the assets.

When it is allowed by applicable law and procedures to use the device(s) of a suspect for a seizure, take into consideration that in some cases it could happen that the device(s) first should be checked for other traces like fingerprints, DNA, and blood traces. This will depend on the case to be investigated.

Before seizing, another good practice is to check the balance of the wallet. If the balance is zero, there will be nothing to seize.

3.3 Desktop Wallet

3.3.1 Introduction

Desktop or software wallets are installed on a computer and provide users complete control of the public and private keys and thus the funds. Examples are Bitcoin Core, Electrum, Exodus, Coinomi, Jaxx Liberty, Atomic and many more. Some of these wallets can be paired with their mobile version.

3.3.2 Bitcoin Core and difference from "light wallets"

Bitcoin Core is the original Bitcoin wallet, and it is still one of the safest places to store bitcoins.

Almost 99% of the Bitcoin network consists of Bitcoin Core nodes (https://coin.dance/nodes).

The big difference from other wallets is that Bitcoin Core downloads the complete history of all bitcoin transactions (the blockchain) and because of that, the wallet does not have to rely on third party nodes to query the balance of the addresses that are in the wallet. On the other hand, a light node (like Electrum, Ledger, Jaxx, etc.), must connect to a full node (like Bitcoin Core) to interact with the blockchain. In other words, once a light client starts up, it connects to a full node (somewhere in the Bitcoin network) and asks the balance of its Bitcoin addresses.

A disadvantage of Bitcoin Core is that it needs some extra hard disk space, especially if the user needs the complete blockchain (+300 Gb) in local storage. Optionally, Bitcoin Core users can activate "Pruning" and thus use a smaller version of the full blockchain. The wallet does this by deleting the older data that it no longer requires while downloading the latest blockchain.

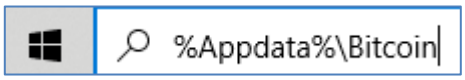
Wallet.dat

The actual wallet file of Bitcoin Core is called wallet.dat, which is the default name. This file contains the private keys, public keys, scripts (which correspond to addresses), key metadata (e.g., labels), and the transactions related to your wallet. Just remember that wallet.dat is the default name. Users can edit it if they want, e.g., "recipes.txt".

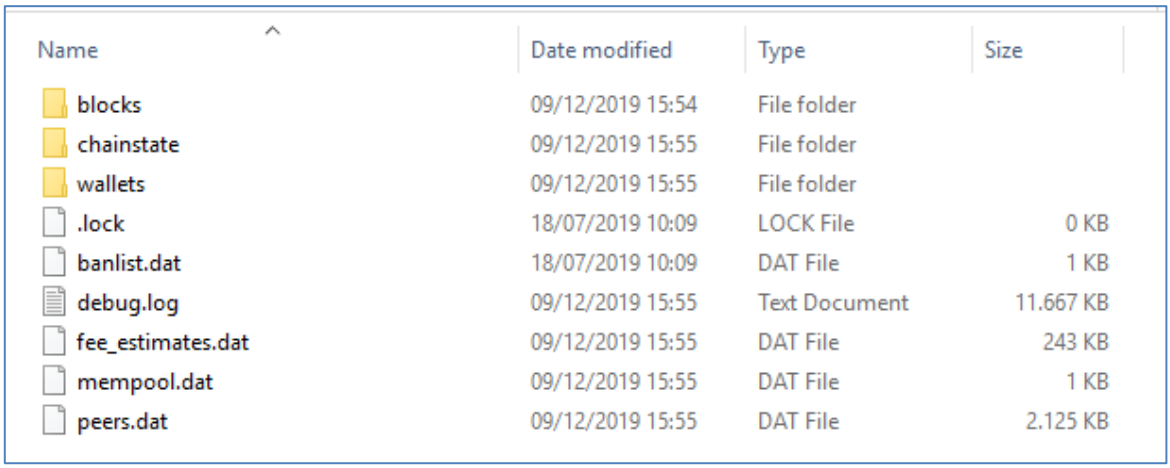
The default locations of the wallet file:

Windows

Go to Start -> Run (or press WinKey+R) and run: %APPDATA%\Bitcoin



Bitcoin's data folder will open:

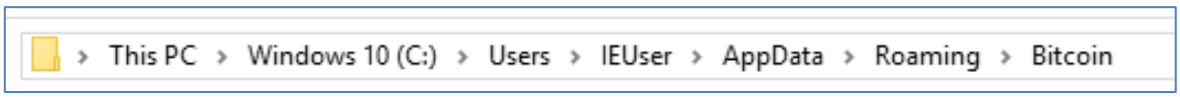


Name	Date modified	Type	Size
blocks	09/12/2019 15:54	File folder	
chainstate	09/12/2019 15:55	File folder	
wallets	09/12/2019 15:55	File folder	
.lock	18/07/2019 10:09	LOCK File	0 KB
banlist.dat	18/07/2019 10:09	DAT File	1 KB
debug.log	09/12/2019 15:55	Text Document	11.667 KB
fee_estimates.dat	09/12/2019 15:55	DAT File	243 KB
mempool.dat	09/12/2019 15:55	DAT File	1 KB
peers.dat	09/12/2019 15:55	DAT File	2.125 KB

For most users, these are the following locations:

C:\Documents and Settings\YourUserName\Application data\Bitcoin (Windows XP)

C:\Users\YourUserName\Appdata\Roaming\Bitcoin (Windows Vista, 7 and 10)



"AppData" and "Application data" are hidden by default. Bitcoin data files can also be stored in any other drive or folder.

Linux

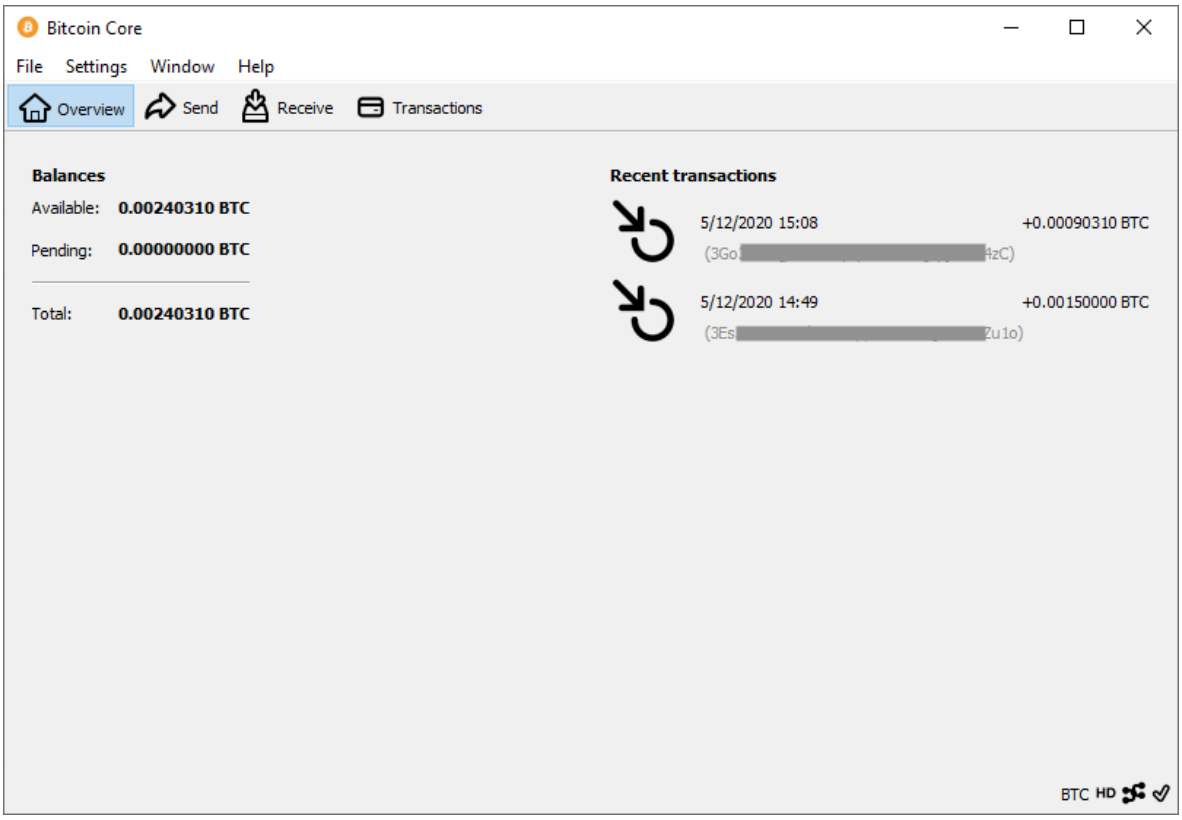
By default, Bitcoin will put its data here: ~/.bitcoin/

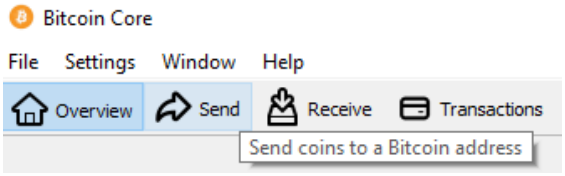
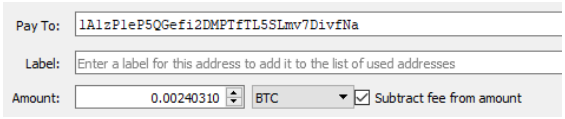
You need to do a "ls -a" to see directories that start with a dot.

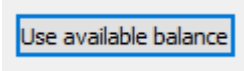
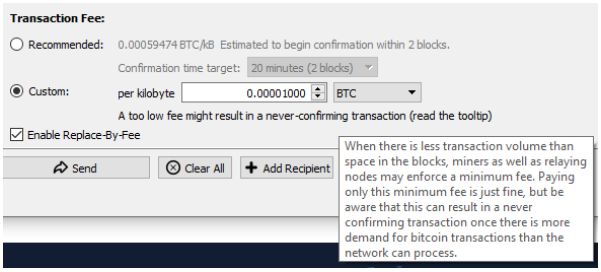
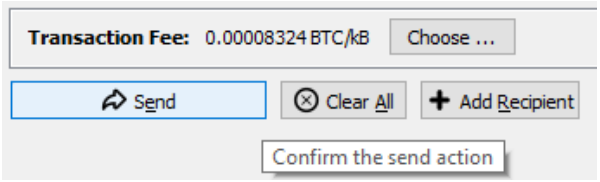
Mac

By default, Bitcoin will put its data here: ~/Library/Application Support/Bitcoin/

Seizing in Bitcoin Core



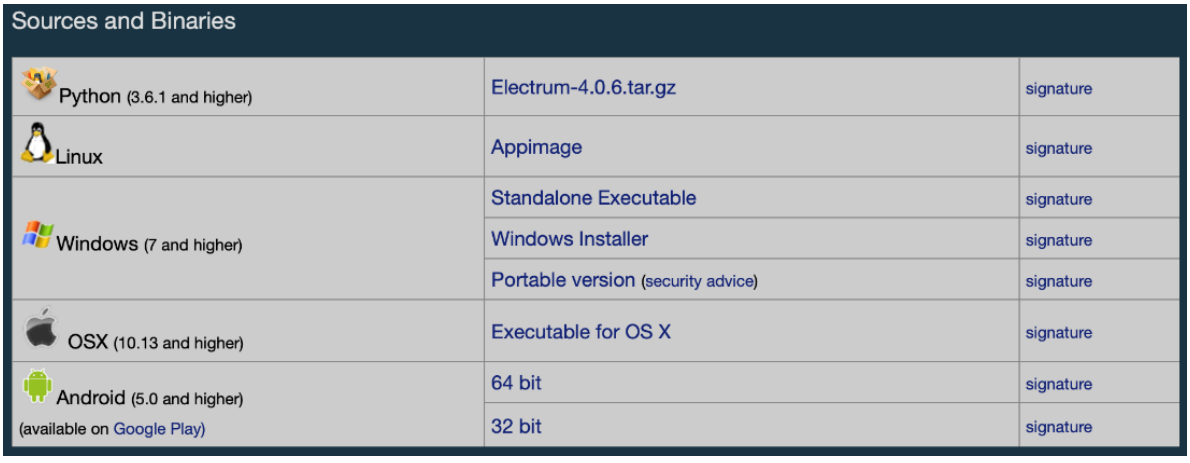
	An encrypted wallet (file) has a padlock in the below right corner. If you do not know the password, no further action is possible.
	If the wallet is not encrypted or you do have the password, click on "Send" to seize the bitcoins.
	In the "Pay To" field, paste the seizing address and check "Subtract fee from account. This fee will be deducted from the amount being sent.

	Click "Use available balance" to send all bitcoins to the government-controlled address.
	If a speedy transaction is necessary, use a higher transaction fee by clicking on "Custom". If there is time and possibility, check https://www.buybitcoinworldwide.com/fee-calculator for estimated fees.
	Hit "Send" to seize.

3.3.3 Electrum

- Uses seed: Mandatory 12-word seed phrase with optional BIP39 extension
- Uses password: Optional

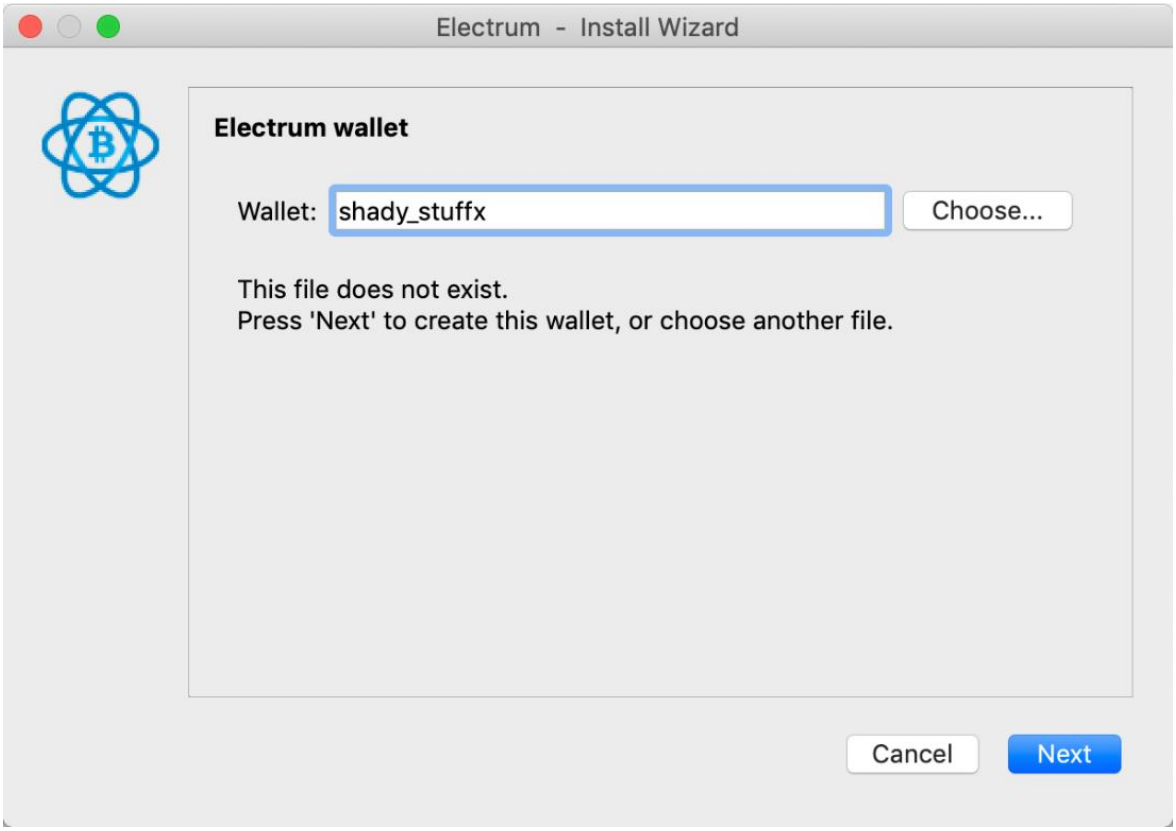
Installing Electrum wallet is quite straight forward. It is available as a mobile app (Android) and a desktop wallet for various platforms (see picture below). Electrum wallet and Exodus wallet (explained later) are very popular.



Tip: When installing and updating an Electrum wallet, it is a good practice to verify its GPG signatures to make sure that you are not installing for example a falsified version containing malware. How to do this can be found at https://electrum.org/#download under topic: "How to verify GPG signatures".

On the official website of Electrum there is a warning for users that Electrum versions older than 3.3.4 are susceptible to phishing and to not download Electrum from another source than electrum.org and learn to verify GPG signatures.

When installing Electrum, you will be asked for a wallet name as seen below. You should be aware that it can be named anything, not necessary "default_wallet". The wallet on the screenshot below is named "shady_stuffx".

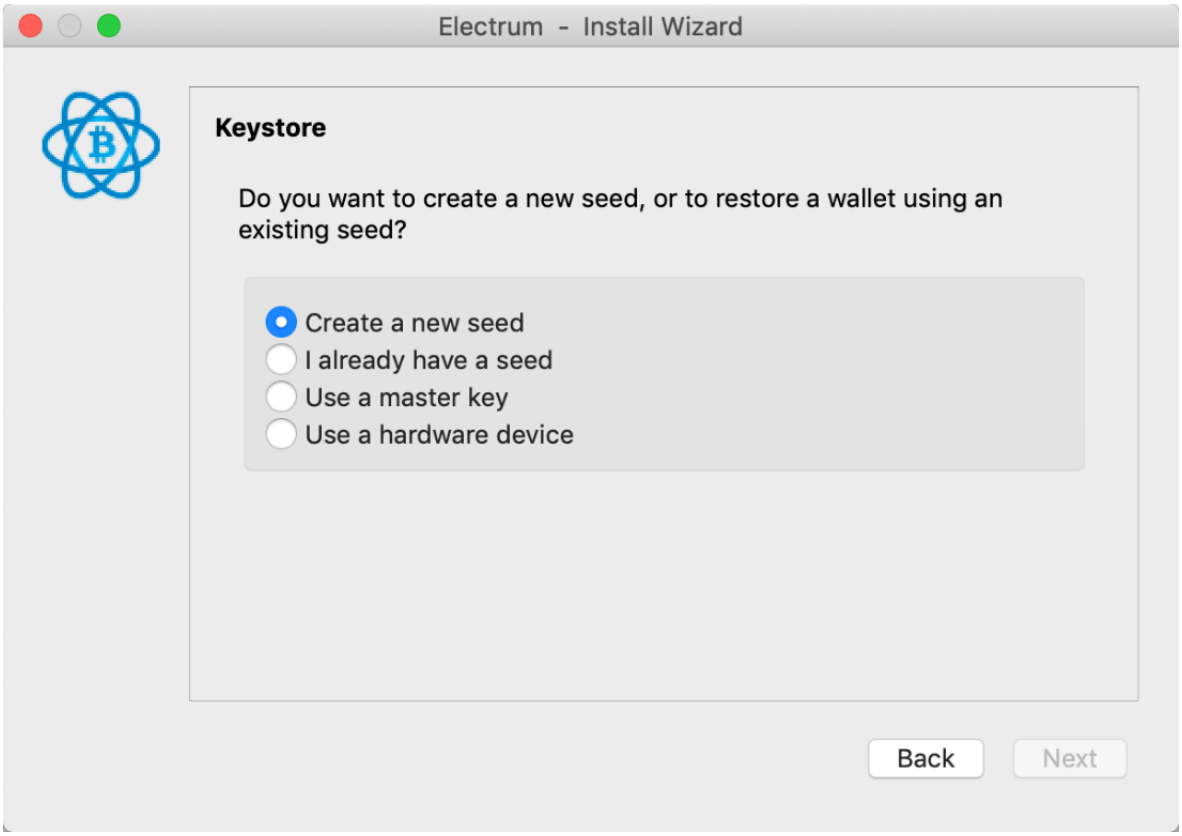


During the installation process, the following types of wallets can be created: standard wallet, wallet with two-factor authentication, multi-signature wallet or an option to import Bitcoin addresses or private keys, as shown below.

Remark: In this Electrum section (including the seizing example) we only cover the use, the seizing and the recovering of an Electrum standard wallet. For wallets with two-factor authentication and multi-signature wallets other requirements apply. We refer to the official Electrum website for more information about these. Two-factor authentication (2FA) is covered later in this guide.

After selecting the option "Standard wallet", you can create a new seed phrase, restore an existing wallet from a seed phrase (see below), use a master key or connect Electrum with a hardware device, as shown below.

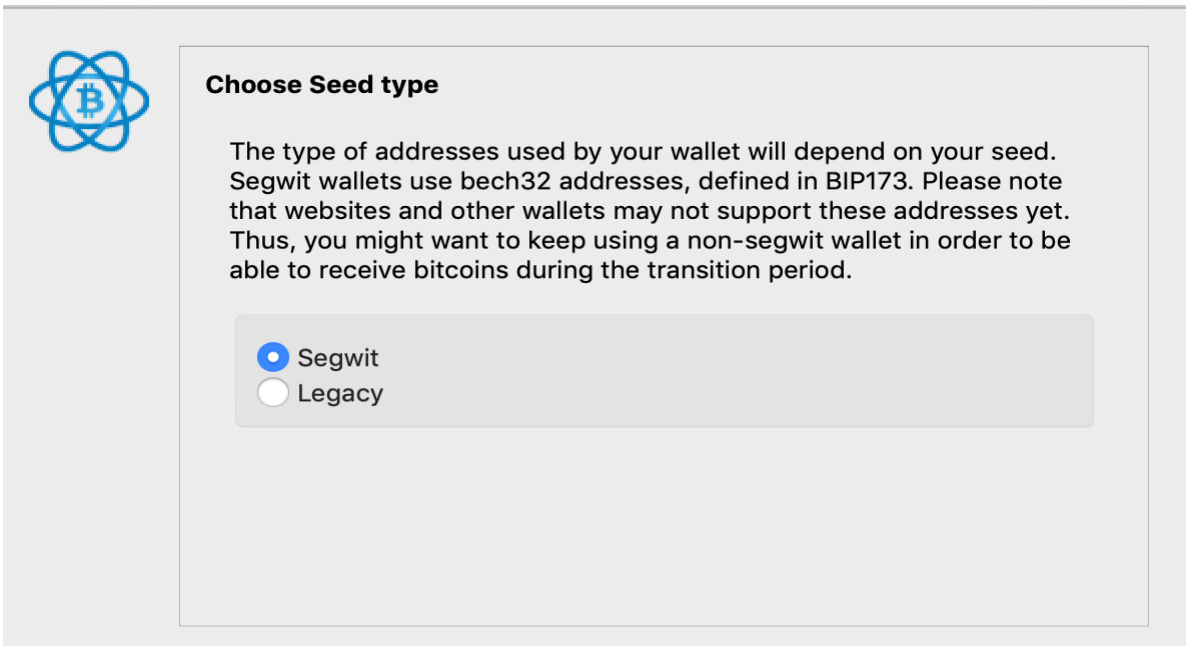
To restore an existing wallet from seed words at this stage you need to select the option "I already have a seed" and input the words you have found.


Electrum - Install Wizard
Keystore
Do you want to create a new seed, or to restore a wallet using an existing seed?
Create a new seed
I already have a seed
Use a master key
Use a hardware device
Back
Next

After selecting the option "Create a new seed", you can choose between two seed types: "SegWit" or "Legacy". Within Electrum, SegWit wallets use bech32 addresses starting with "bc1" and legacy wallets addresses starts with 1.

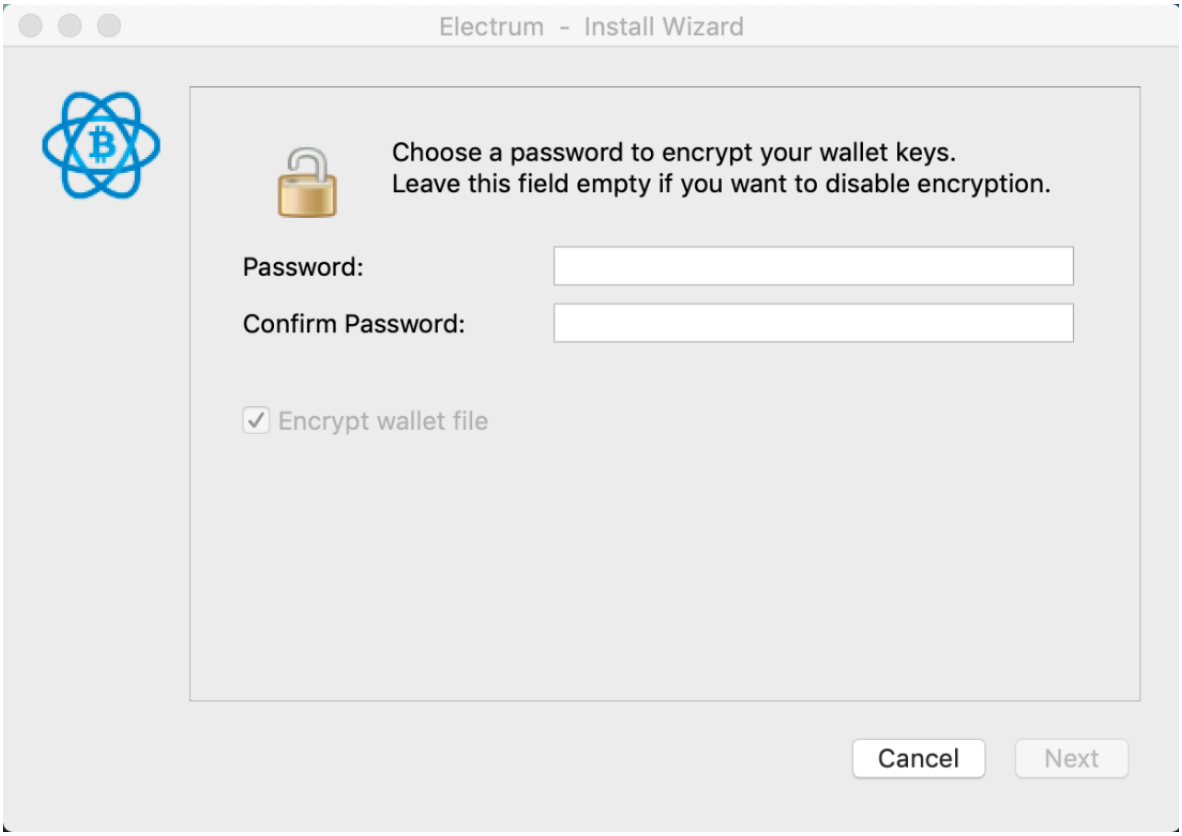
As remarked in the screenshot below please note that some websites and wallets may not support these bech32 addresses yet and that you might keep using a non-SegWit wallet.

An example of such a wallet is Jaxx Liberty which is covered later.

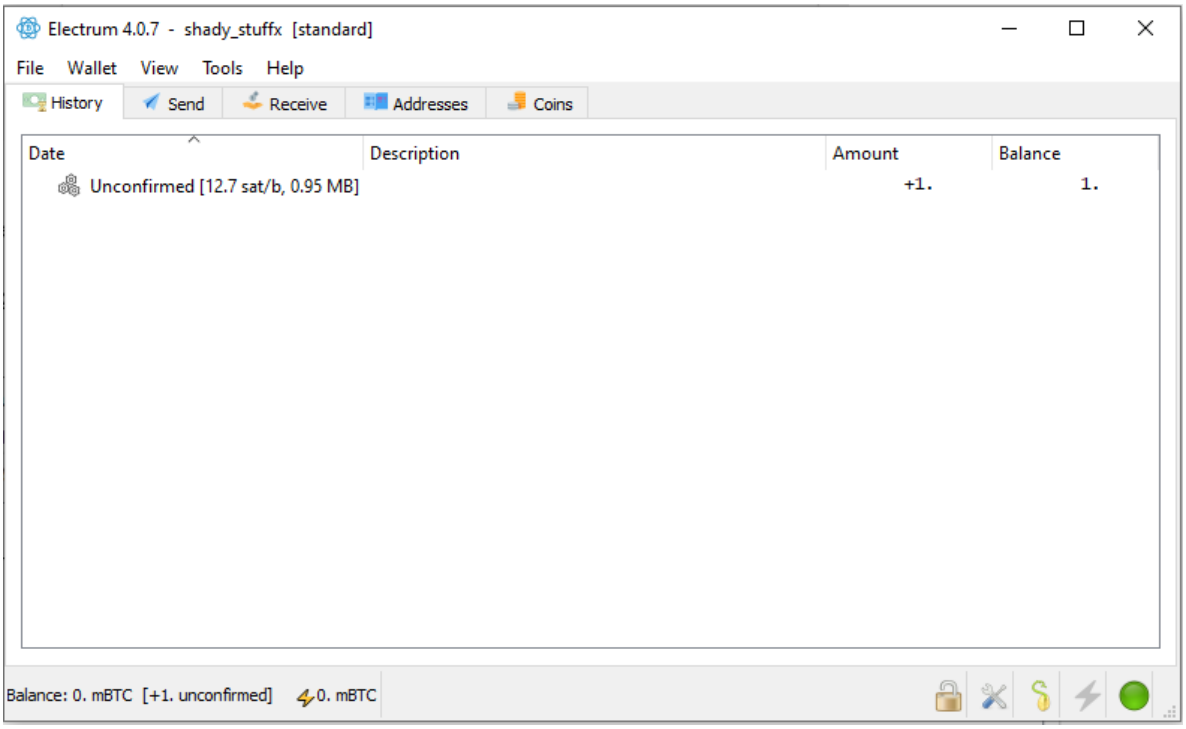

Choose Seed type
The type of addresses used by your wallet will depend on your seed. Segwit wallets use bech32 addresses, defined in BIP173. Please note that websites and other wallets may not support these addresses yet. Thus, you might want to keep using a non-segwit wallet in order to be able to receive bitcoins during the transition period.
Segwit
Legacy

Now, when creating a new wallet, you will receive a new seed phrase. Electrum uses typically 12 words which can be extended with some custom words. In this example, the seed word list is "airport sort ahead toe mixture idea hollow drum keen bargain second awesome".

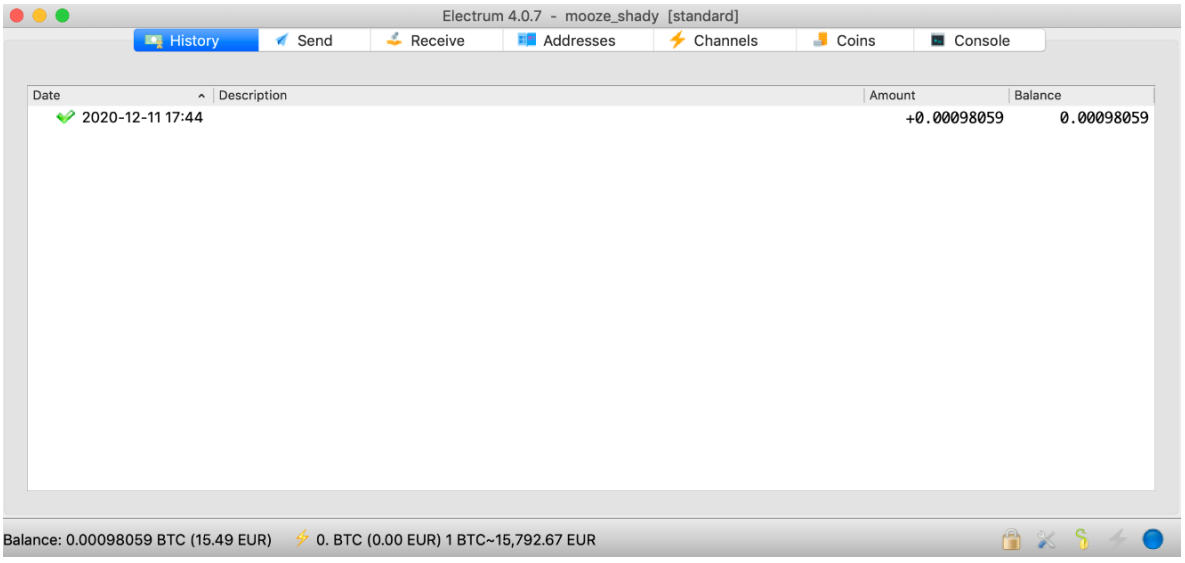
Finally, the user will be able to add a password to the wallet, as shown below. If a password is added, the wallet file will be encrypted.



From the main page of Electrum wallet as shown below, you can see the wallet name "shady_stuffx", version, history of transactions and balance (in this example unconfirmed, meaning the wallet is receiving a pending transaction).


Electrum 4.0.7 - shady_stuffx [standard]
File Wallet View Tools Help
History Send Receive Addresses Coins
Date Description Amount Balance
Unconfirmed [12.7 sat/b, 0.95 MB] +1. 1.
Balance: 0. mBTC [+1. unconfirmed] 0. mBTC

Thus, when Electrum is running on the Desktop, it looks like the screenshot below, even if the Mac and Windows version look cosmetically a bit different all the functions are done in the same way. Immediately, you notice the available balance and the transactions that happened (in this example case, only one incoming transaction).


Electrum 4.0.7 - mooze_shady [standard]
History Send Receive Addresses Channels Coins Console
Date Description Amount Balance
2020-12-11 17:44 +0.00098059 0.00098059
Balance: 0.00098059 BTC (15.49 EUR) 0. BTC (0.00 EUR) 1 BTC~15,792.67 EUR

Observe that the wallet has a padlock (icon) in the bottom right corner. When the padlock is closed then the wallet is password protected and encrypted and a password will be needed to transfer/seize funds. To extract the private keys or to obtain the seed phrase from this wallet, a password will be required too.

If the padlock is open, then the wallet is not (password) protected. The funds can be seized without a password.

Below two screenshots (Mac and Windows) where the padlock is zoomed. Next to the padlock icon is the "Preferences" icon, followed by "the Seed", "Lightning Network" and "Network" icons. When clicking on the "Seed" icon a password will be requested to obtain the seed phrase (if the wallet is encrypted).

Encrypted wallet = closed padlock (Mac)

Unencrypted wallet = open padlock (Windows)

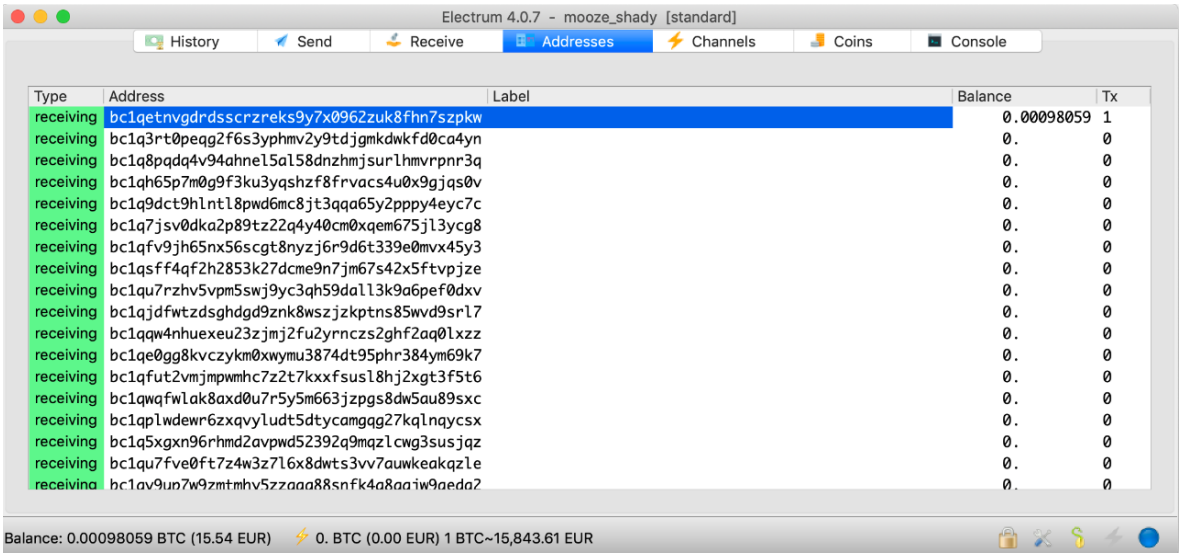
The wallet depicted above has only one incoming transaction and a total balance of 0,00098059 BTC which represented 15,49 EUR at the time of the screenshot. The "Balance" can be found at the bottom and the name of the wallet at the top, which is in this case a standard wallet named "mooze_shady". The version of the wallet is 4.0.7.

Below the name of the wallet, you can find the following tabs:

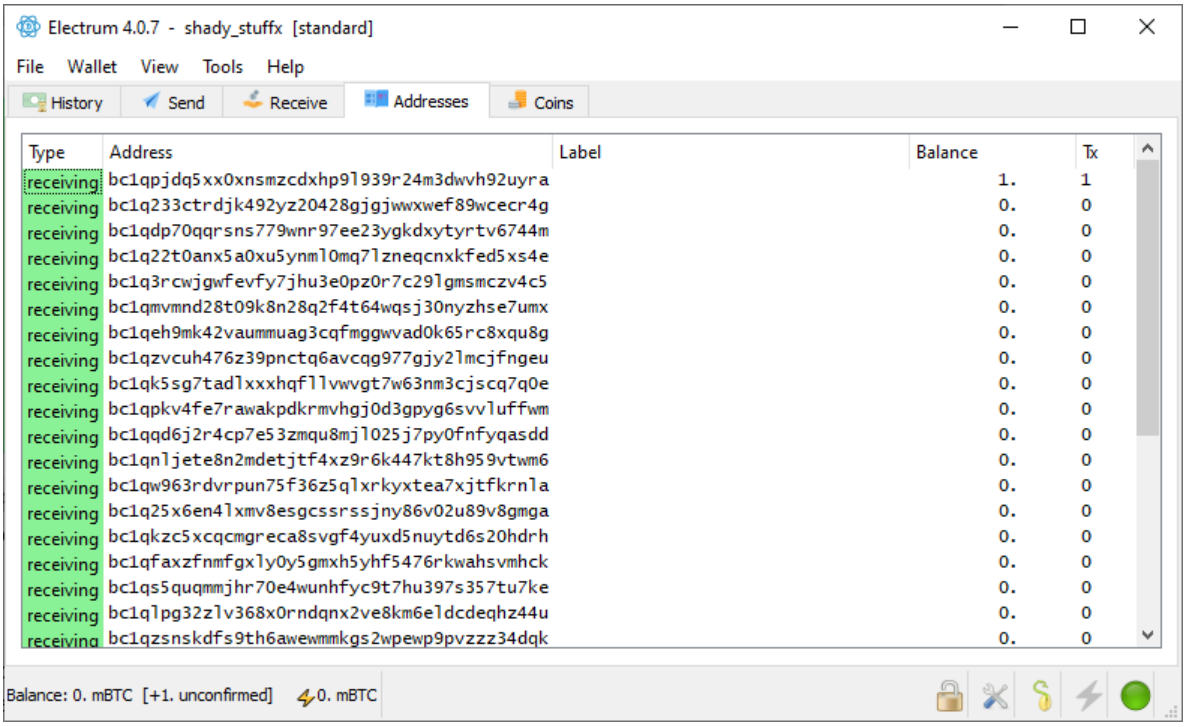
- History
- Send
- Receive
- Addresses
- ...

The "History" tab contains an overview of the transactions (see above). This overview of transactions can be very relevant to conduct further investigations (such as blockchain analysis). Also, when you right-click on a transaction more details about this transaction can be obtained. But blockchain analysis is out of the scope of this guide.

The "Send" tab will be used to send bitcoins and to seize them. The "Receive" tab is used to receive bitcoins. The "Addresses" tab contains a list of bitcoins addresses that are belonging to this wallet.



Above: addresses screenshot on a Mac computer.



Above: addresses screenshot on a Windows computer.

In this case, in the Mac screenshot only the bitcoin address "bc1qetnvgdrdsscrzreks9y7x0962zuk8fhn7szpkw"[25] has a balance. In the Windows screenshot only the address "bc1qpjdq5xx0xnsmzcdxhp9l939r24m3dwvh92uyra" has an unconfirmed balance, but if you look closely the Windows wallet is set to mBTC whereas the Mac wallet is in BTC. These wallets are created for training purposes, and hence only have a single used address. Often, several bitcoin addresses will have a balance which will be summed up in the balance total at the bottom.

[25] i.e., a Segwit wallet use bech32 address, defined in BIP173

Seizing example (on Mac, similar for Windows)

Seizing example (on Mac, similar for Windows)

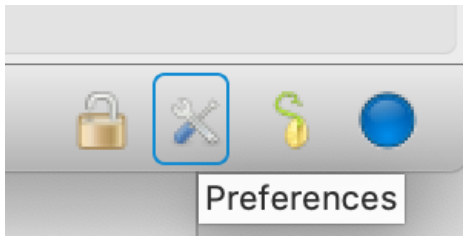
ATTENTION: **Uncheck** "Use Replace-By-Fee"!

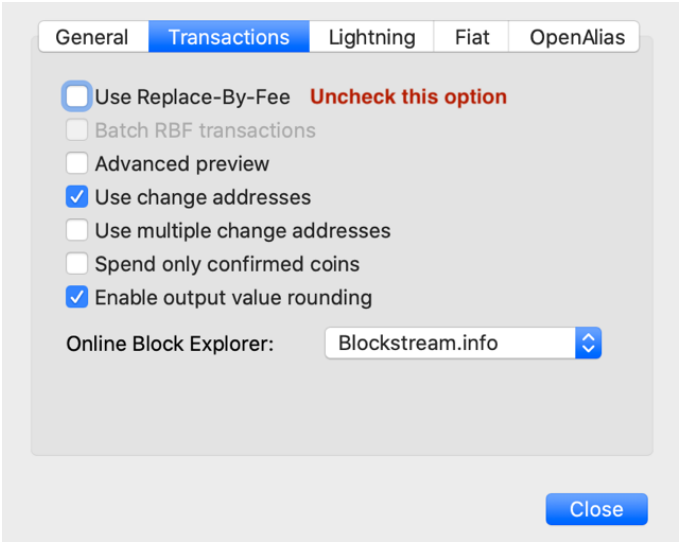
Since Electrum version 4.0.4, users are able to cancel a Bitcoin transaction before it is confirmed, provided that the Replace-By-Fee option is activated in their wallet (before that transaction was submitted to the network).

To cancel a transaction however, the user must have enough balance in the wallet.

Remark: The Replace-By-Fee option is activated by default.

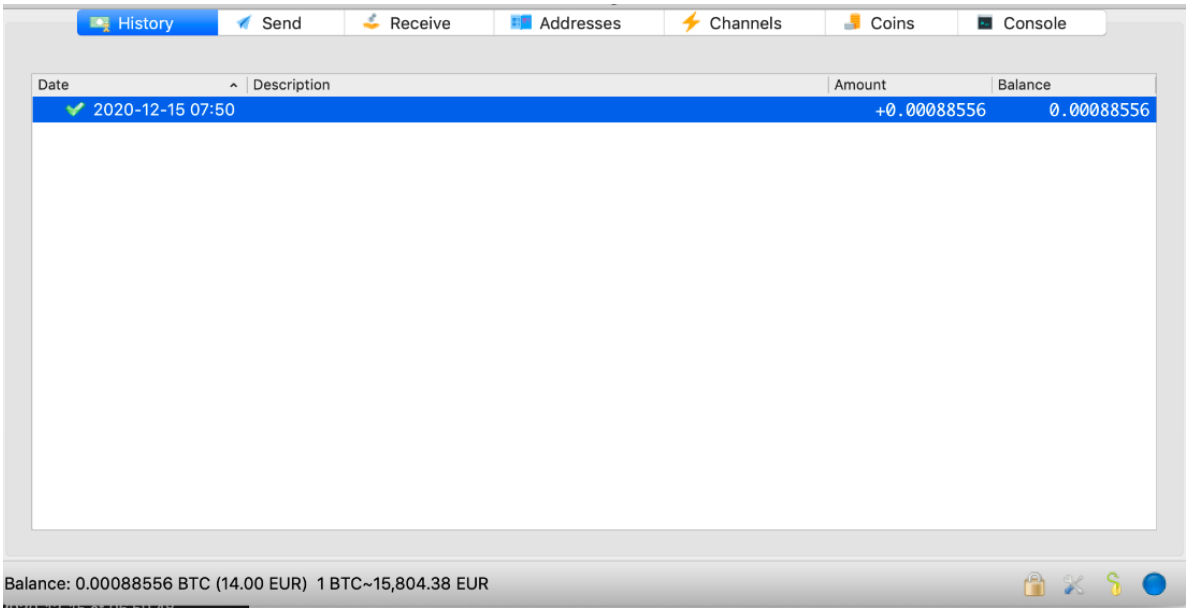
To exclude all possible risks, it's a good practice to uncheck the "Use Replace-By-fee" box as depicted below:





Once it's deactivated, we can continue the seizing.

Below you can find an example of a step-by-step seizure from an Electrum wallet (version 4.0.7) containing 0,00088556 BTC (equivalent to 14,00 EUR).



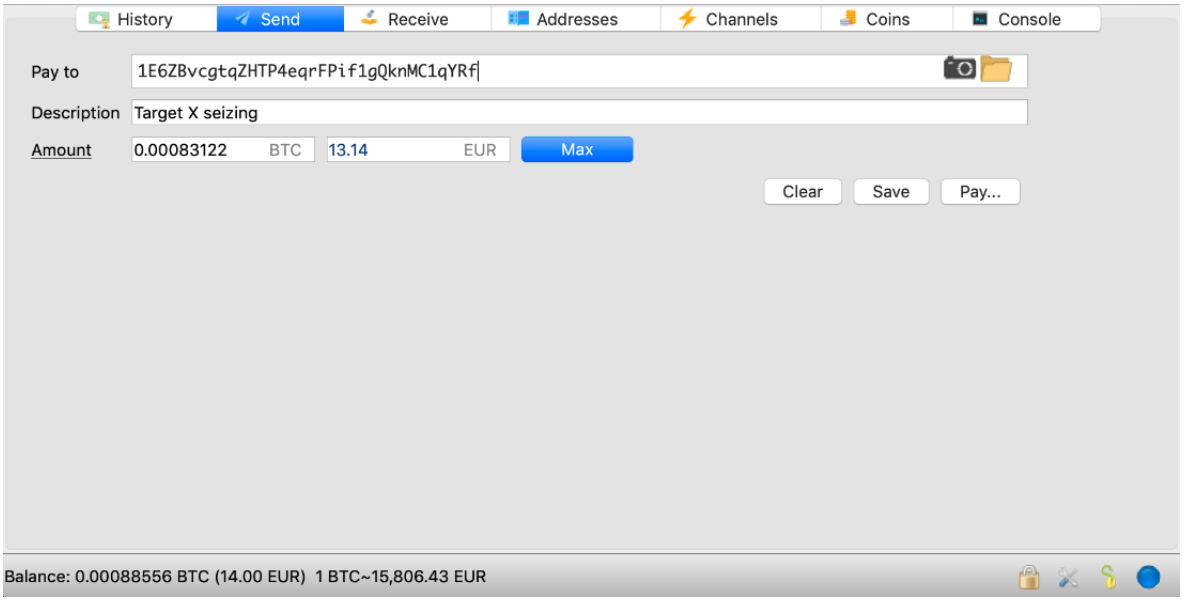
On the "Send" tab as depicted below, it is demonstrated how the bitcoins (i.e., 0,00088556 BTC) in this wallet will be transferred and seized to a government-controlled wallet.

Next to "Pay to" you must fill in the seizing address by manually typing or copy-pasting it. But be very cautious for typos. A good practice when typing the address is to create and empty notepad file and have at least 2 or 3 different persons type in the address in notepad. Also make sure that others cannot see the previous typing. Once all 2 or 3 persons have typed the address on different pages in notepad compare this 2 or 3 typing's to each other, when all of them match, then you can be sure that everyone agrees on the address where the bitcoins will be sent.

To the far right of this "Pay to" input field there are two more options, "Read QR code" and "Read file". With the QR code option a bitcoin address represented as a QR code can be read. This QR code (representing a seizing address) can be printed in advance or be stored on a mobile device such as a smartphone.

Whatever option you may choose, always double-check the correctness of the seizing address before the seizure and it is recommended to handle conform the four-eyes principle as mentioned before under the pre-seizure planning section.

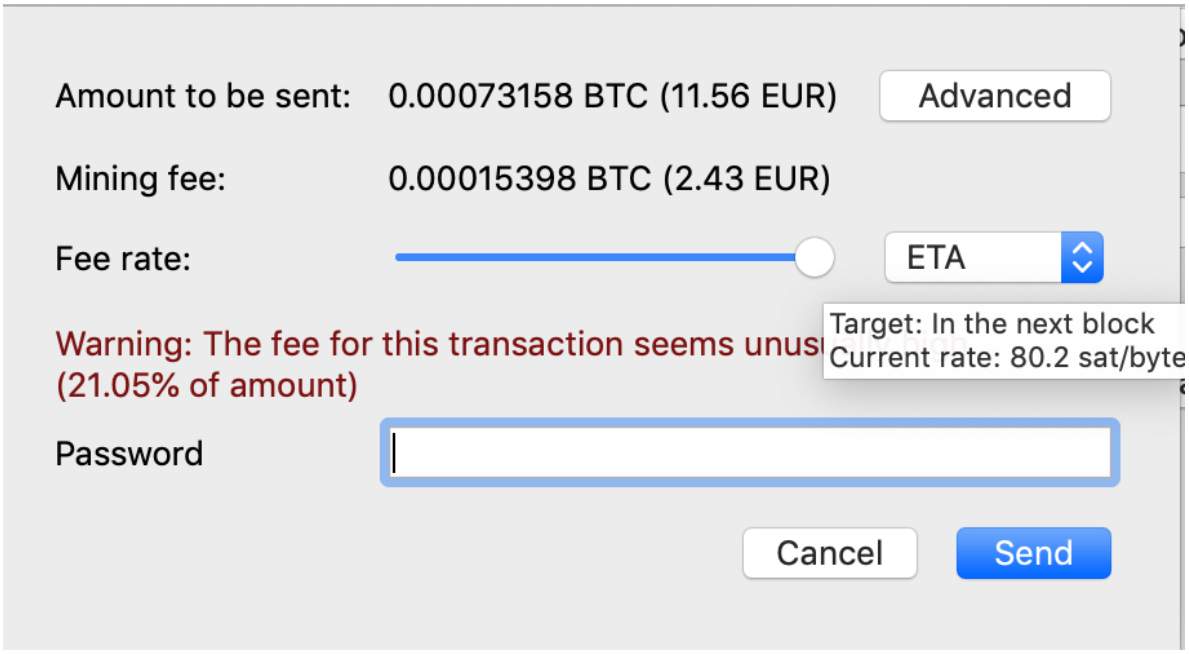
A local description (e.g., target name, case number) to the seizing transaction can be added. The amount must set to "Max" to seize the complete wallet (meaning all funds within the wallet possibly residing on different bitcoin addresses).



Next, after clicking on "Pay..." in our specific example the window as shown below appears.

The fee estimation algorithms (ETA, Static or Mempool) and fee rate slider setting could look differently depending on how the Electrum wallet was used in previous (send) transactions on the suspect's computer.

In our example (after clicking on "Pay...") the fee calculation algorithm is set by Electrum to "ETA", and the slider is set by Electrum uttermost right (maximum). The fee estimation algorithms and fee rate slider setting can be adjusted (see below).



Note that **the fee is dependent on the bytes of the transaction** (not the bitcoin price, but it naturally correlates to it indirectly), one input and one output being the cheapest to send since it uses the least amount of bytes from the bitcoin block in the blockchain. Depending on network congestion it might be quite expensive like in this example. Normally the fee is within cents of dollars. But since it has more to

do with the bytes of transaction the fee can vary a lot. It is recommended to estimate the transaction fee from a Bitcoin fee calculator (described later in the manual) before making the transaction.

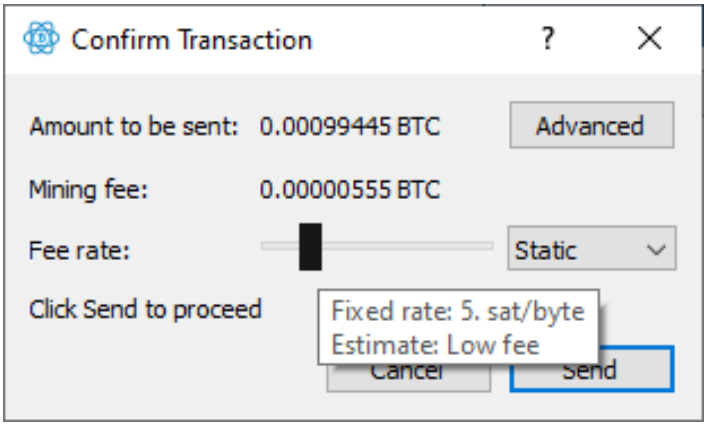
In the screenshot above there is a warning that the fee for this transaction seems unusually high (21,05% of amount!). In fact, with this actual fee settings it is targeted that our example seizing transaction will be added in the next block of the blockchain.

As mentioned before, transaction fees are costs which are paid to the miners.

Remark that this is a very high fee which can be adjusted depending on specific (tactical) criteria regarding the case and other relevant elements such as the applicable legal framework and seizing procedures. Some relevant questions regarding (the amount of) transaction fees to think about before a seizure are:

- Who will pay this fee? (Suspect? Government?)
- If there is a risk that the funds need to be reimbursed in a later stage to the suspect because he or she is unguilty who will take these costs on his account? And in this latter case how much needs to be reimbursed to the suspect?
- Are there any accomplices in play (see hereafter)?
- ...

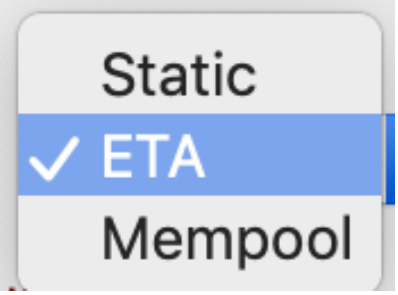
For example, concerning specific (tactical) criteria, whenever there is a high risk that an accomplice during a police intervention or even the suspect after a given time (e.g., short after a house search) can have access to the targeted wallet (e.g., through its private key(s) or a seed phrase), then a risk analysis (cost-benefit analysis) should be made to decide in which block this transaction can be targeted (next block, within 5 blocks etc.). Also, as mentioned above, depending on the applicable legal framework, and seizing procedures check on whose account the transaction fees will be charged to avoid any discussion afterwards.



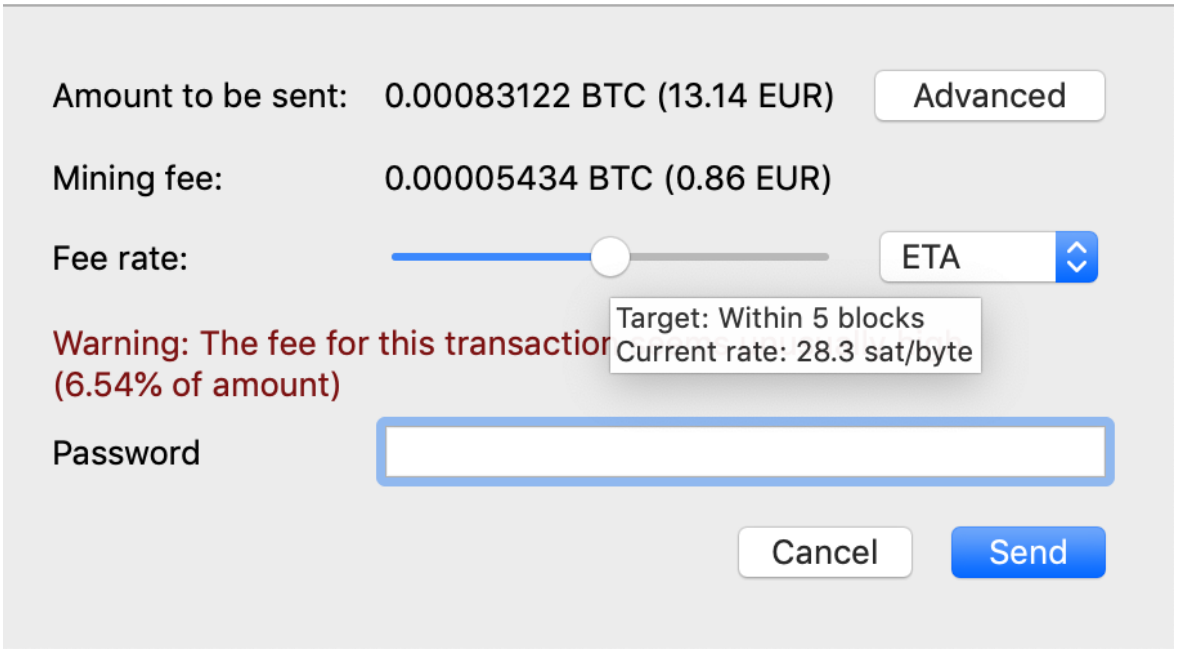
Another example when sending the transaction is to set a fixed (static) fee and in the above screenshot, a transaction of 5 satoshis per byte is set and the transaction should go through in hours based on the current network traffic.

As mentioned before and depicted below, there are several fee estimation algorithms in the selection list next to the slider: Static, ETA and Mempool. Static is a fixed rate and does not take market conditions into account. ETA and Mempool suggest suitable fees based on fee market conditions. In the case of ETA when pausing the cursor over the fee slider you will get a tooltip indicating within how many blocks the transaction will be confirmed. On average it takes 10 minutes to mine a block. In case of Mempool it will be the size of unconfirmed transactions that pay more.

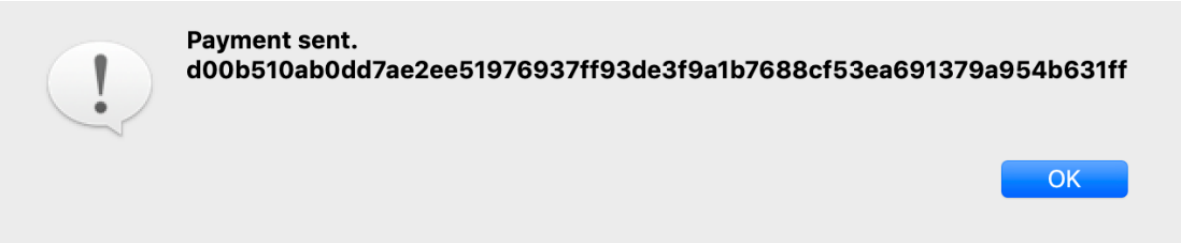
More information can be found at: https://bitcoinelectrum.com/how-to-manually-set-transaction-fees/



For each fee estimation algorithm option, the fee slider can be adjusted. Below as another example for the option "ETA" the fee slider is moved to the left (less or more halfway). In this case, it is targeted to confirm and record the seizing transaction within 5 blocks in the blockchain and the cost is now 6,54 % of the amount. Note again, that the percentage seem high since the network at time of writing is very congested due to the record highs in Bitcoin price. Also remark that the more to the left you drag the slider the lower the fee but the longer the transaction takes to confirm, and the opposite is true for the right side.



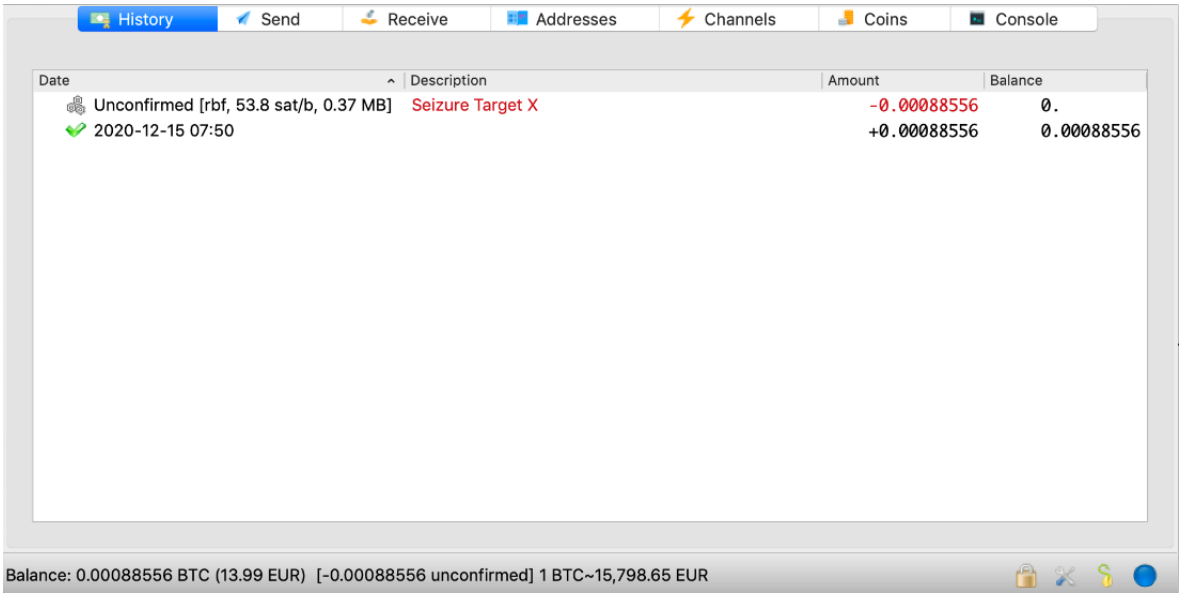
If the wallet is password protected and encrypted, a password will be required to effectively seize the funds. After entering the password click "Send" and the payment will be sent as depicted below.



The alphanumeric number in the above screenshot refers to the hash or "Transaction ID" of this seizing transaction. Using this number, the status of the transaction can be checked within the blockchain

through a blockchain explorer e.g., https://www.blockchain.com/btc/tx/d00b510ab0dd7ae2ee51976937ff93de3f9a1b7688cf53ea691379a954b631ff

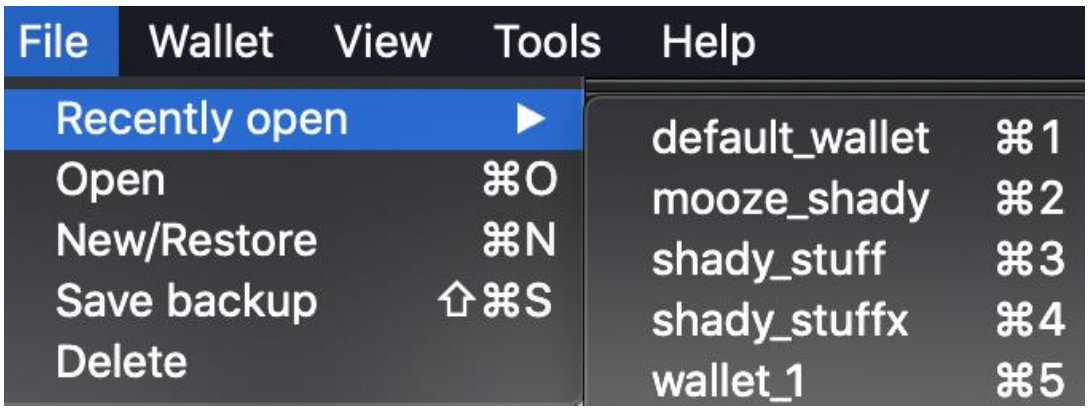
Immediately after this seizing transaction, the transaction history of our seized wallet looks as follows:



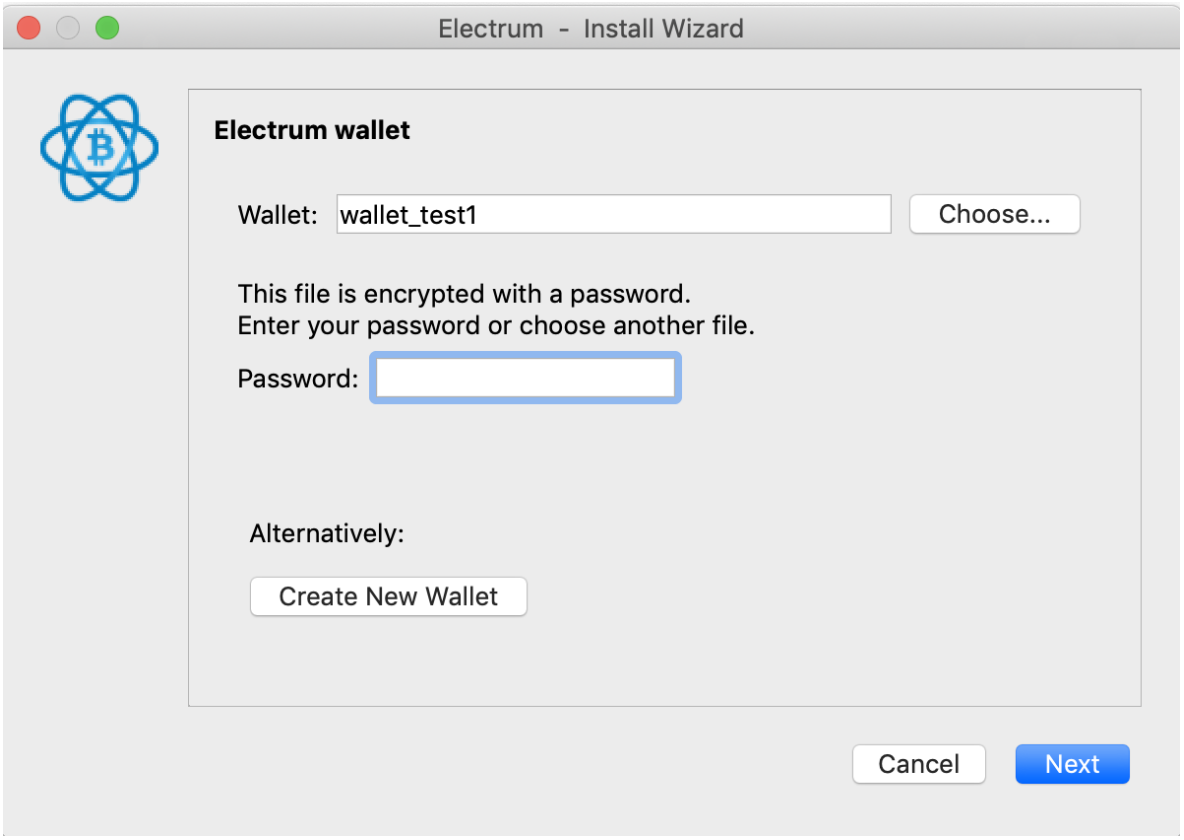
As you can see, the seizing transaction is still unconfirmed.

Some important remarks

- There cannot be any test transaction made before the actual seizure. If the criminals use a shared wallet there might be safeguards in place if an unauthorized transaction is noticed.
- Seizing is time critical and the seizure transaction must be made in one transaction and with a relatively high fee so others cannot replace the transaction while waiting to be processed (mined into a new block) in the Mempool.
- When Electrum is open on a computer it is a good practice to check (if allowed by law and applicable procedures) if there are any other existing Electrum wallets on the same computer. As showed in the example below when selecting from the Electrum menu "File" > "Recently open" you will see that this computer contains at least 5 different Electrum wallets.



And even better, when clicking on "Open", you will be directed to a "wallets" folder which in our example contains eight Electrum wallets. One of these wallets is named "wallet_test1" (this wallet is not listed under "Recently open" as depicted above) and is also password protected as you can see in the screenshot below. When a wallet is password protected and encrypted, not only for executing a transaction, a password will be required to also open this wallet.

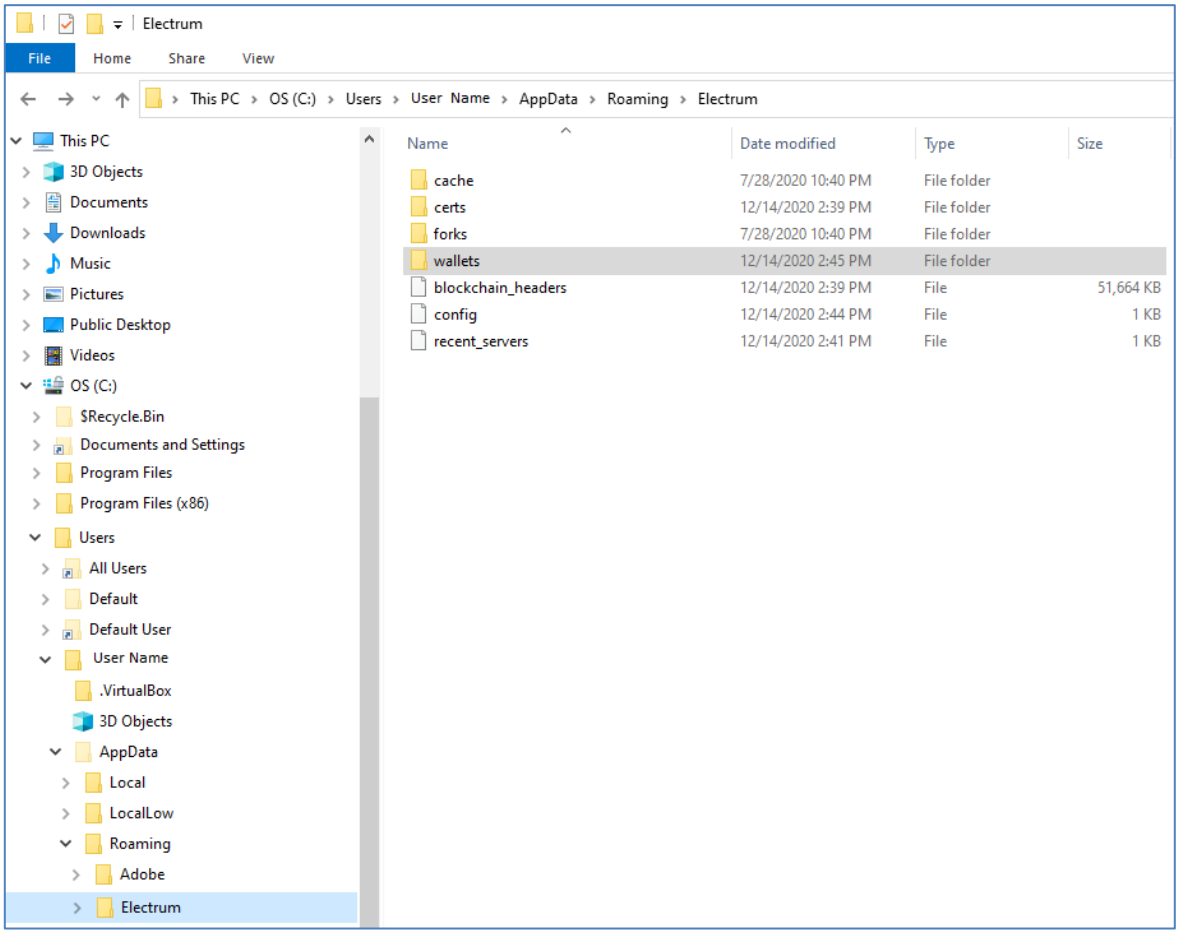


Be aware that a suspect can store Electrum wallets at any place on his computer. Also, a computer can contain different wallet software. If allowed by law and applicable procedures in your country, on a Windows computer, the running processes can be checked using Task Manager for instance (CTRL+ALT+DEL). Also, you can check the computer for the presence of wallet software through its icons (e.g., on the Desktop) etc.

The default locations of the wallet file(s):

Windows

- Show hidden files (see above)
- Browse to: Users\YourUserName\AppData\Roaming\Electrum\wallets



Linux

By default, Bitcoin will put its data here: ~/.electrum

You need to do a "ls -a" to see directories that start with a dot.

Mac

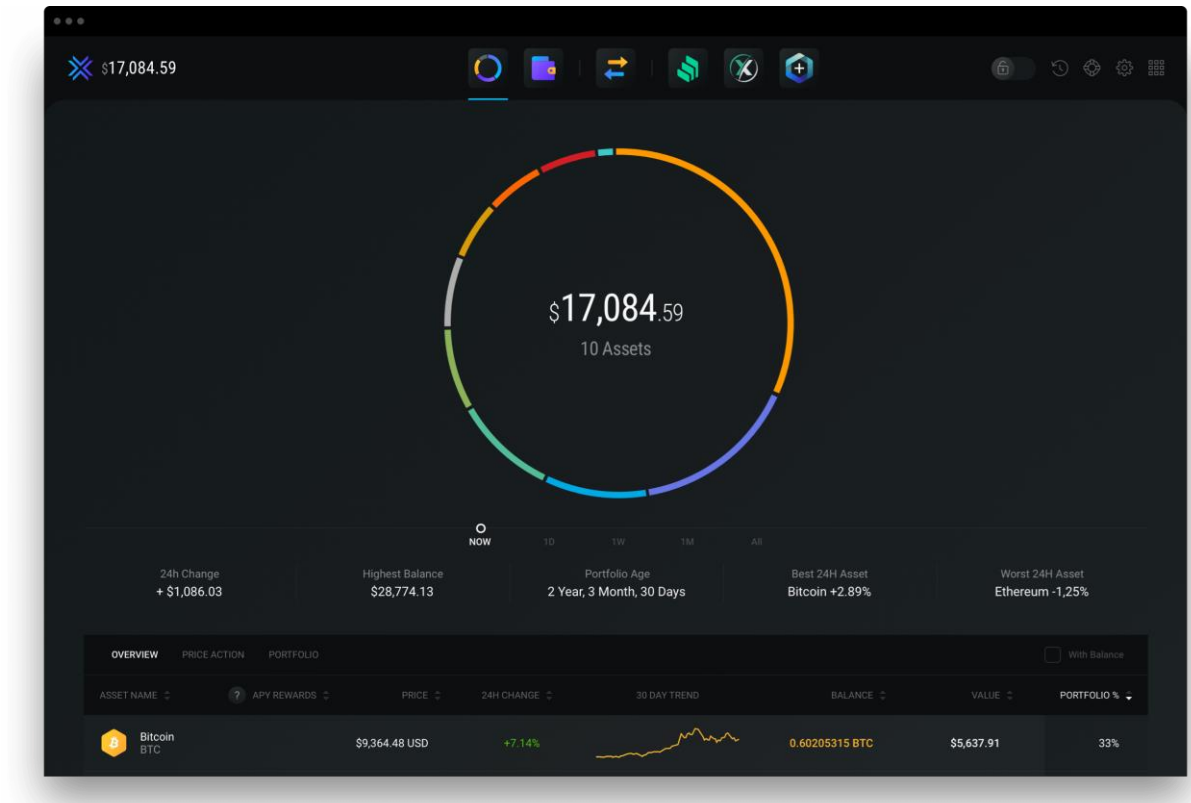
- Open Finder
- Go to folder (shift+command+G) and type ~/.electrum

A password protected and encrypted standard Electrum wallet can be bypassed when finding its corresponding seed phrase. This wallet can then be restored through the Electrum installation wizard and when the wizard asks, "Do you want to create a new seed, or to restore a wallet using an existing seed?" then the option "I already have a seed" should be selected (as shown below) and in the next step the found seed phrase can be entered. Hereafter, this wallet will be restored through its seed phrase. Optionally, a new password can be chosen for this restored wallet. From this restored wallet, a seizure can be made.

Electrum - Install Wizard
Keystore
Do you want to create a new seed, or to restore a wallet using an existing seed?
Create a new seed
I already have a seed
Use a master key
Use a hardware device
Back
Next

3.3.4 Exodus

- Uses seed: a 12-word seed phrase can be used (compatible with MetaMask, Jaxx Liberty, and more)
- Uses password: yes (only for accessing the wallet)
- Exchange function: yes



Exodus is a popular multicurrency wallet that supports more than 120 cryptocurrencies and tokens. Users can exchange funds to other cryptocurrencies in the wallet itself.

Be aware that this wallet (once accessed with a password) can go to "auto-lock". The user can define this in the settings and can be configured between 5 minutes and 2 hours (or never).

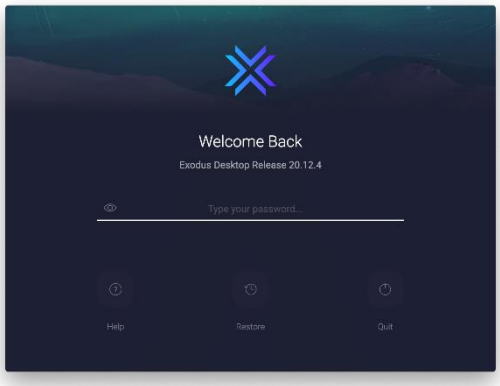
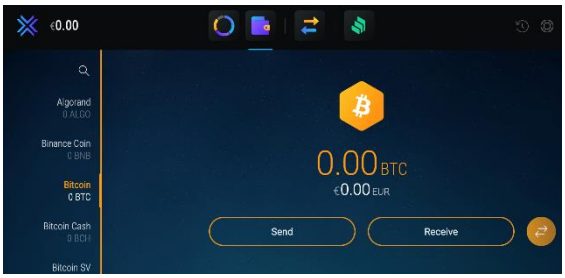
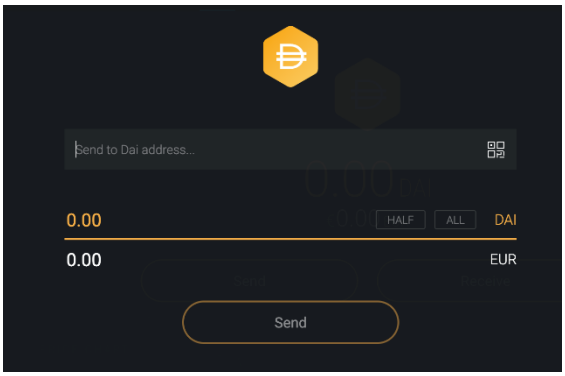
The Desktop wallet can be paired with a mobile version and users can even pair it with a Trezor hardware device. Trezor (Model T or Model One) will keep its private keys offline for extra security.

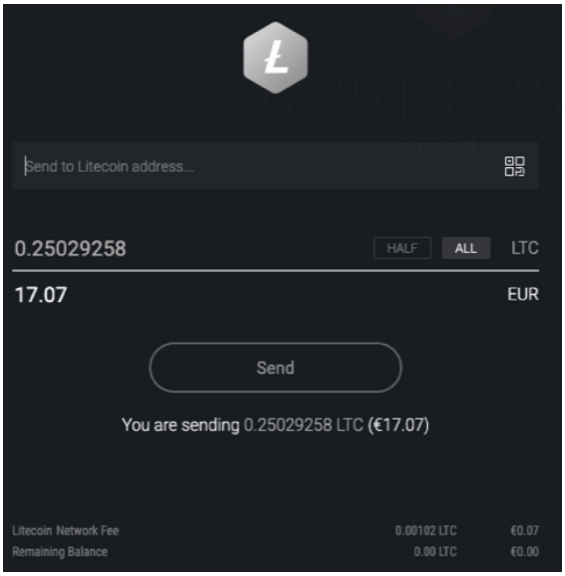
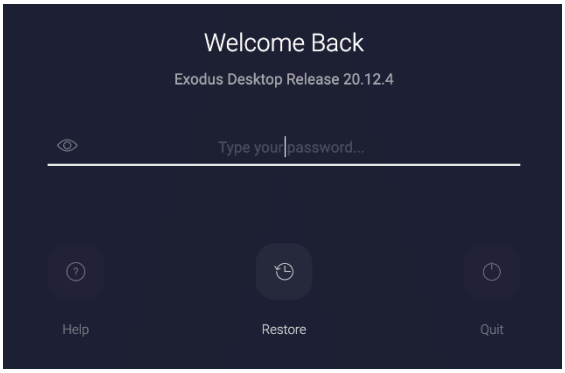
Assets that do not have a zero balance cannot be hidden (however this can be done in Jaxx Liberty).

Note that when doing in wallet swaps to other cryptocurrencies there are floating minimums and maximums[26].

[26] For more information, please refer to: https://support.exodus.io/article/787-how-do-i-exchange-assets-in-exodus#

Seizing in Exodus (Desktop version)

	When starting up Exodus, a password is needed to access the wallet. When no password is found (or the suspect will not cooperate), there is no further way to seize funds. The only option is to find the seed phrase and restore the wallet with it.
	When the wallet is accessed, click on one of the cryptocurrencies that have funds. In a multicurrency wallet, each cryptocurrency must be seized separately. For Ethereum tokens, first send the tokens, afterwards send Ether (ETH) itself.
	For example: DAI DAI is a stable coin on the Ethereum network that attempts to maintain a value of $1.00 USD. This means you need an Ethereum address to seize DAI tokens. Again, when dealing with Ethereum tokens, first send the tokens, afterwards send Ether (ETH) itself.

	This screenshot shows some Litecoin in the wallet. Click "ALL" to send the maximum available. Transaction costs are shown at the bottom of the app. FYI: Of course, this part of the seizing would need a Litecoin address. New Litecoin address formats start with M, LTC1 (bech32) while old formats started with 3 (which was too confusing with a Bitcoin address). If you like to swap Litecoin to Bitcoin in the wallet, please check if allowed by your country's legislation and keep in mind there are minimums and maximums on these swaps.
	In case a seed was found When a seed was found, you can use it to restore the wallet.
	Type the 12-word secret phrase in order with no capital letters. Click the arrow to the right when finished. After a few seconds, Exodus will open with a pop-up "All done!". Click OK and wait a few minutes while Exodus rescans the blockchains and displays the balances.

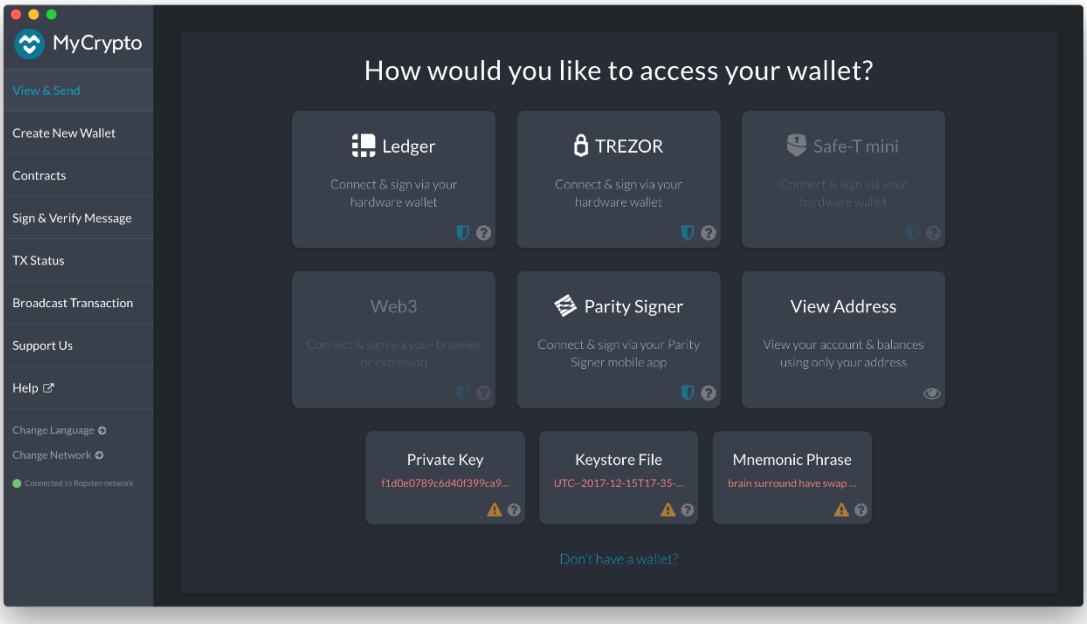
So, for every cryptocurrency to seize, a corresponding government-controlled seizing address will be needed, which can become cumbersome.

E.g., bitcoins need a Bitcoin address, litecoins need a Litecoin address, etc.

3.3.5 Ethereum Wallets

3.3.5.1 MyCrypto Wallet

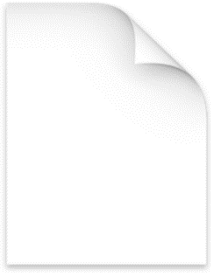
- Uses seed: a 12-word seed phrase can be used (compatible with MetaMask, Jaxx, and more)
- Uses password: yes
- Uses wallet file: optionally, it is called a KeyStore file



The MyCrypto wallet (as well as MyEtherWallet) can be accessed in multiple ways. For instance, you can use it together with a Ledger or Trezor hardware wallet, but users can also create a new wallet file in MyCrypto itself ("Create new wallet").

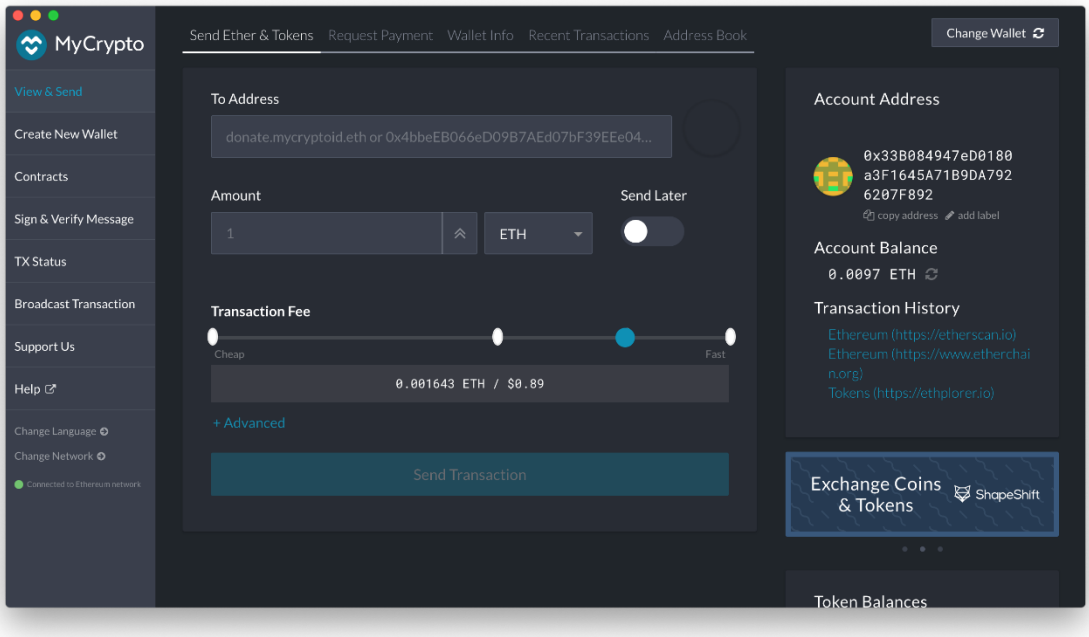
When having access to this wallet on the suspect's machine, it is suggested to click on the "Keystore File" button first, since by default (under condition a KeyStore file was created), it will take you to the right folder where this file is located. Caveat: this file is password protected!

A KeyStore file (example: screenshot below) is an encrypted version of a unique Ethereum private key which is used to sign the transactions. By default, it starts with UTC-- and a timestamp (unless the user renamed the file):



UTC--2020-03-09T11-47-05.877Z-...18facbb021

Document - 489 bytes



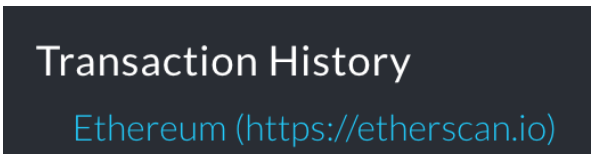
MyCrypto (and other Ethereum wallets) can store both Ethereum (ETH) and Ethereum tokens.

Seizing in MyCrypto

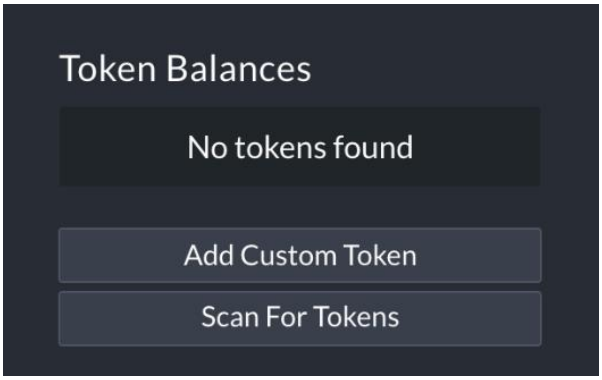
This wallet can be accessed in several ways

- The KeyStore file and the password
- A private key and its password
- A seed (mnemonic phrase)
- A hardware device (Ledger or Trezor) was found, and the PIN-code is known. In this case it is better to use the apps that are native to Ledger and Trezor

Check the Ethereum address on Etherscan.io by clicking on the link and expand the ERC-20 token holding. That way you can see the exact balance and all the ERC-20 tokens that are connected to this address. One Ethereum address can contain several ERC-20 tokens



Back in MyCrypto, click "Scan for Tokens" (bottom right).



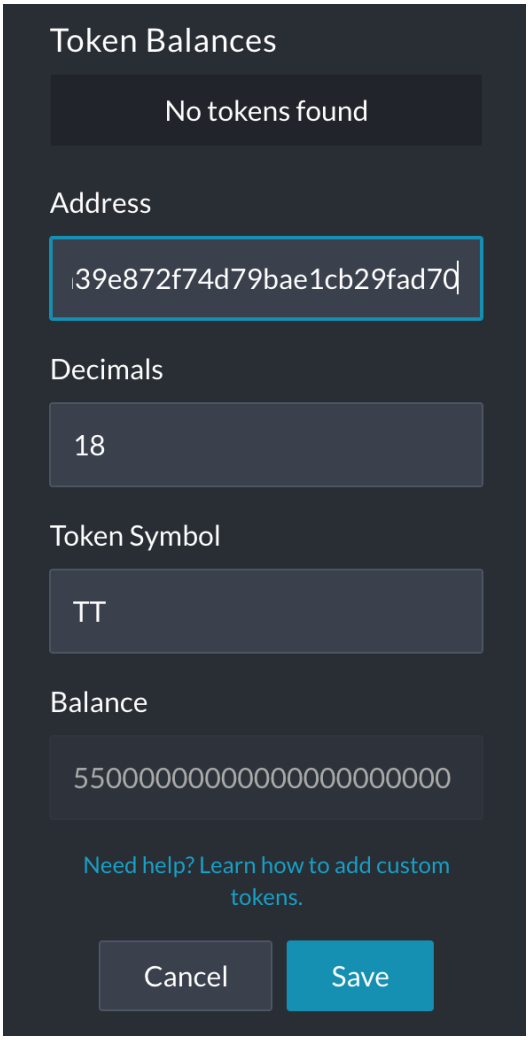
Adding a custom token in MyCrypto

When the Etherscan website shows ERC-20 tokens and MyCrypto does not, you can add them to MyCrypto by clicking on "Add Custom Token".

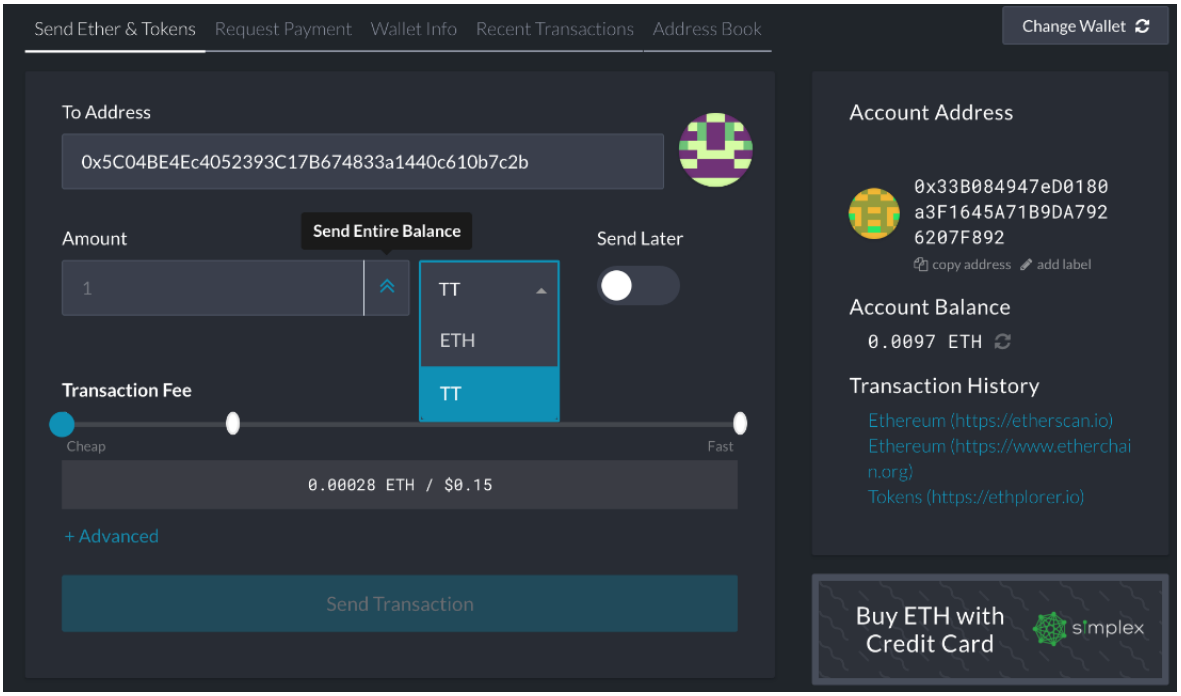
Next, in Etherscan, click on the name of the token you want to add to MyCrypto (in this case, "Training Token")

And copy the contract address of the Training Token

Next, paste this address into MyCrypto by clicking on "Add Custom Token", all fields will be filled in automatically and click Save.


Token Balances
No tokens found
Address
39e872f74d79bae1cb29fad70
Decimals
18
Token Symbol
TT
Balance
55000000000000000000000
Need help? Learn how to add custom tokens.
Cancel
Save

Seizing continued



The first assets that must be seized in an Ethereum wallet, are the Ethereum tokens. This is so because the Ether (ETH) in the wallet will also be used to pay the gas (transaction) price.

In "To Address", fill in the government controlled Ethereum address (it starts with 0x).

Once all tokens are sent to the Ethereum seizing address, the Ether (ETH) itself can be seized. Use the same Ethereum address as the one you have used for the token(s) seizing.

Seizing steps

- Click on the picklist (right to "Amount") and choose the tokens that have to be seized.
- Click "Send Entire Balance", so all tokens will be seized (in the example, all the TT tokens)
- Move the "Transaction Fee" slider to the right for faster transactions (but more expensive)
- Hit the Send Transaction button

Do the same manipulation for every other token and end the seizing with Ethereum (ETH) itself.

3.3.5.2 Metamask

- Uses seed: yes
- Uses password: yes
- Swap function: yes

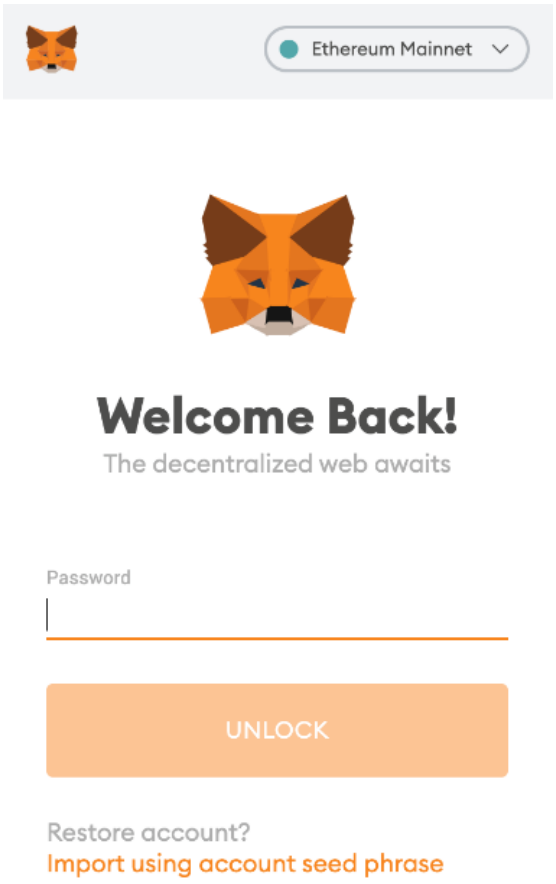
Metamask is available as a browser extension (Fox icon) that serves as an Ethereum wallet[27]. It is also available as a mobile application, but this guide will only cover the browser extension.

Just like in any other Ethereum wallet, users can store Ether (ETH) as well as Ethereum tokens.

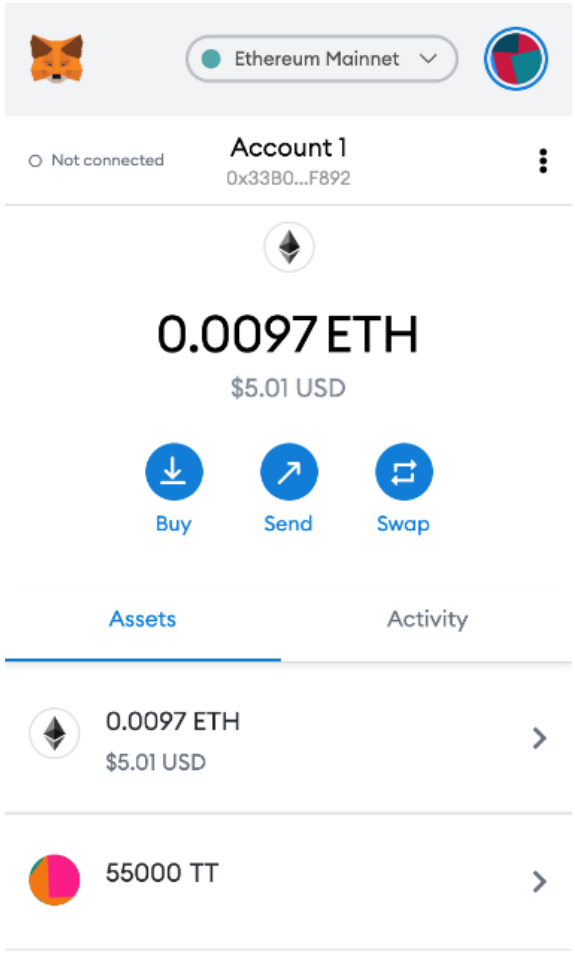
The wallet can also interact with the decentralized applications (dApps), for instance Uniswap (a decentralized exchange) or Compound (a DeFi app).

Seizing in Metamask

Option 1: password was found

	To be able to access this wallet you need a password. A typical Metamask password consists of minimum 8 characters. Alternatively, if you have found a seed phrase but no password, click on" Import using account seed phrase".

[27] More of Metamask refer to https://docs.metamask.io/guide/



Using the password, you will see a similar screen as depicted here.

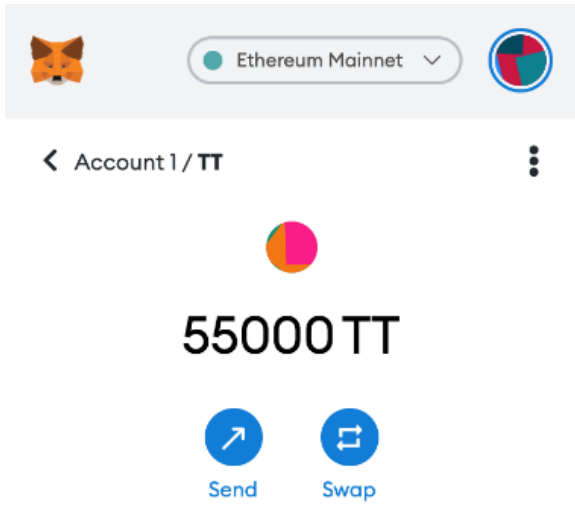
Here you get an overview of the assets that are in this wallet.

As you notice, there are 0.0097 ETH and 55000 TT tokens in the wallet.

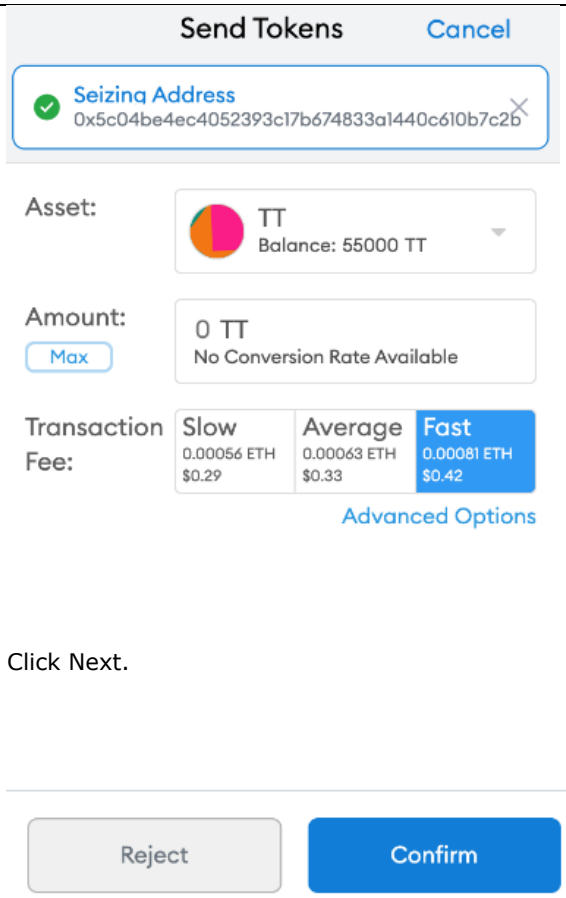
The wallet address of this wallet is mentioned below "Account 1", which is a default name.

If necessary, it can be copied just by clicking on it.

Click on the Menu icon next to the Account (3 points) and click on "View on Etherscan" to be sure you did not miss any important tokens to seize.



If you see any tokens in the wallet, seize them first by clicking on the token and hit "Send" to send these to the government-controlled seizing address. Click "Fast" next to the transaction fee. Fast means "more transactions cost", but you will have a faster confirmation of your transaction.

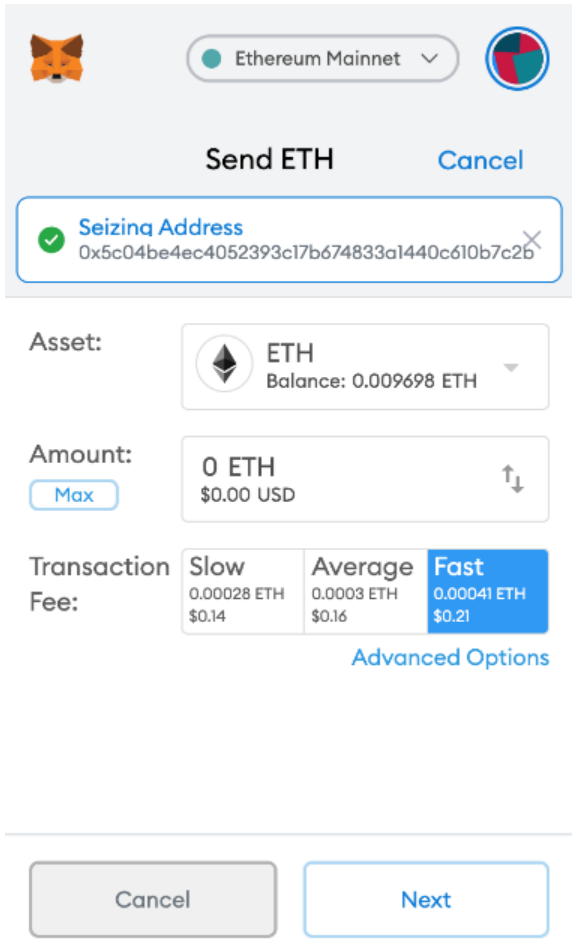


Click Next.

Click Confirm to seize this token.

Every token you find in the wallet must be seized separately to the seize government-controlled Ethereum address.

Be aware that the suspect might have put in place a hidden script that sends cryptocurrencies to an address he controls.



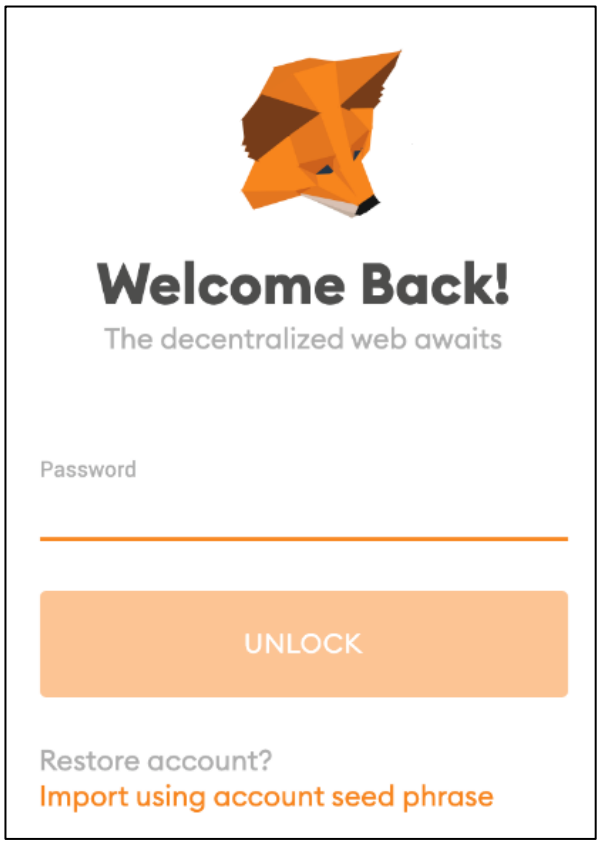
Finally, click on ETH and send the maximum amount of Ethereum (click "Max") to the same seizing address.

Again, click "Fast" next to the transaction fee. It is a bit more expensive but your seized Ether will be faster at their destination (seizing) address.

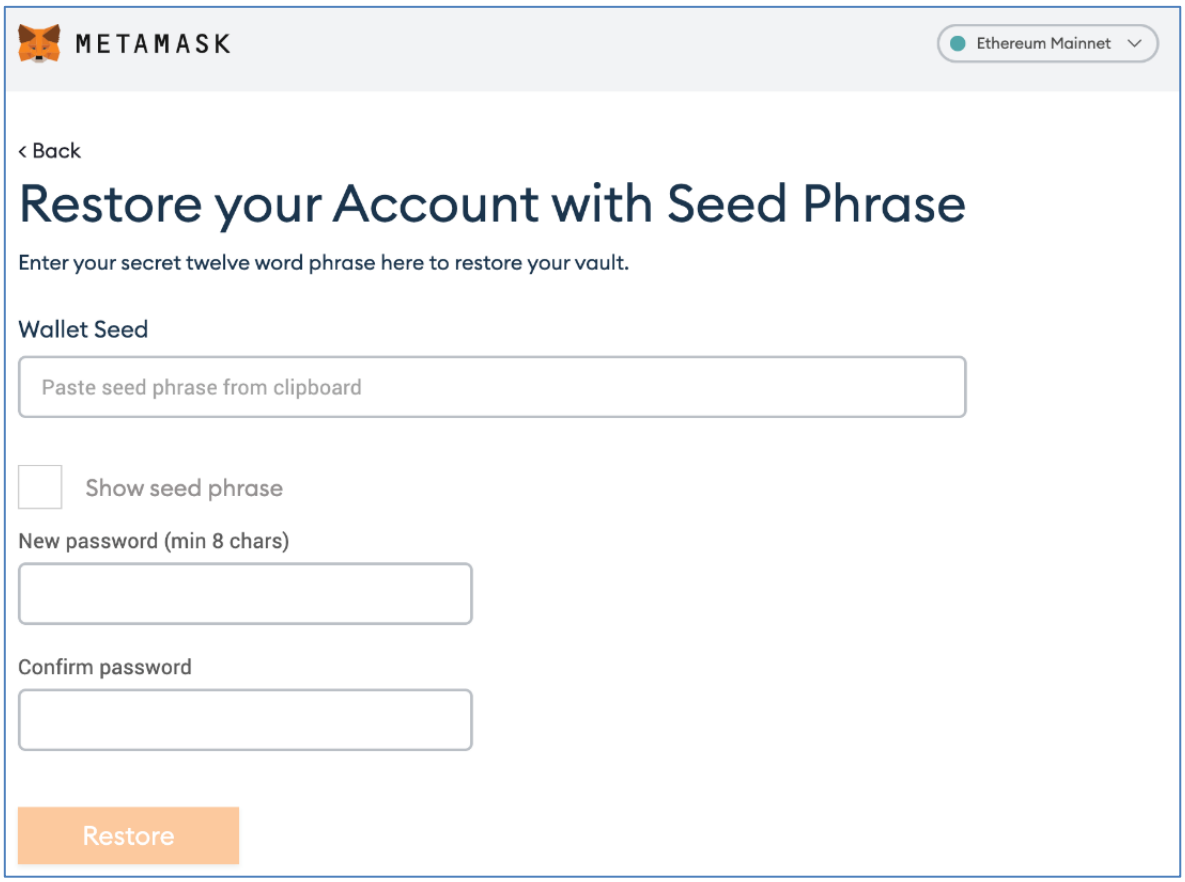
Click Next.

Finally, click Confirm to seize.

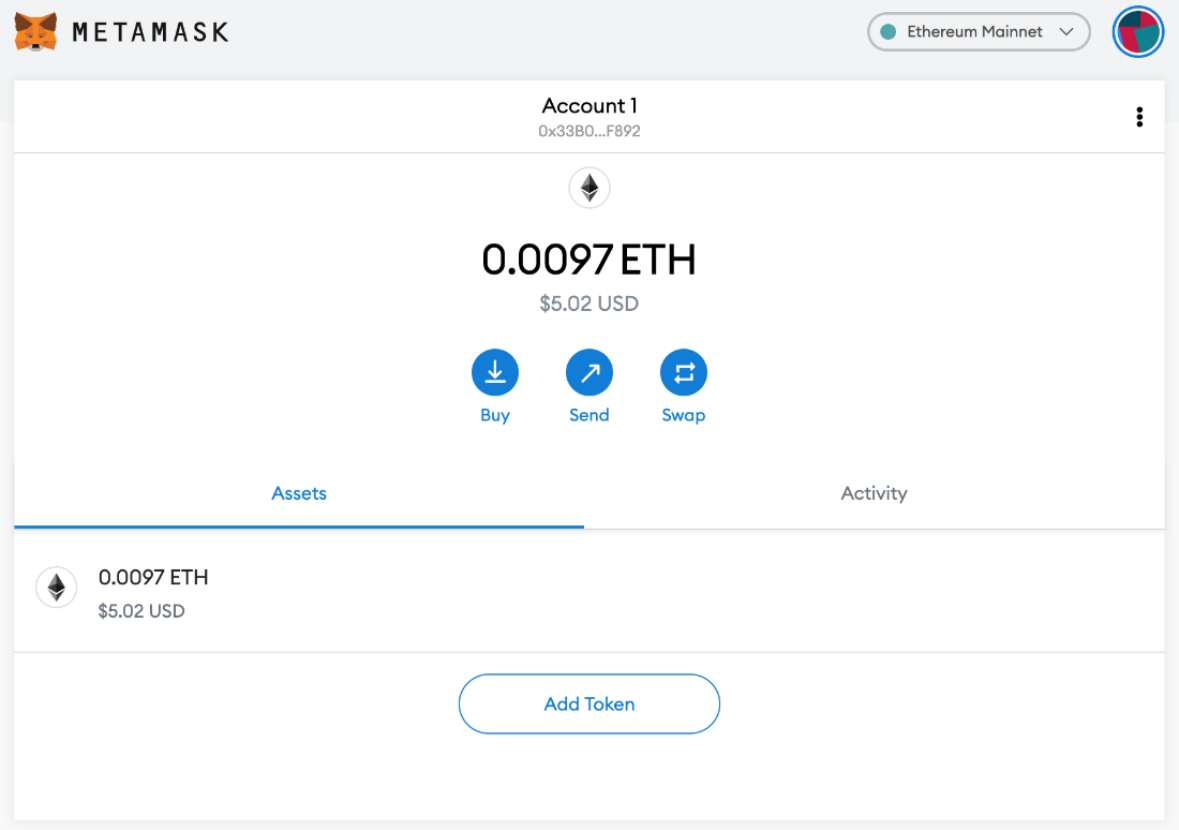
Option 2: only seed was found but no password



If a seed phrase was found at the premises, you can restore the wallet and set your own password. A Metamask seed phrase consists of 12 English words. The seed is compatible with other wallets such as Ledger, Trezor, Jaxx and others. To begin, click on “Import using account seed phrase”.

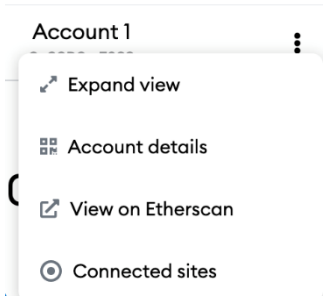
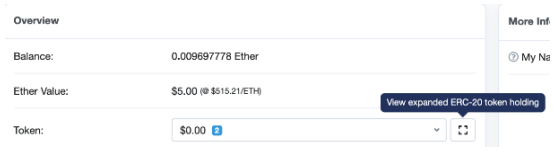


Type in the found seed phrase, give it a new password (minimum 8 characters) and confirm it. Write down the chosen password on a piece of paper.



Next, you will see a similar screen as if you had typed in a password. Seizing can continue as explained above.

Tip: After restoring with a seed, not all tokens might be present in the wallet. You can check this on the Ethereum blockchain (e.g., etherscan.io). Below is explained, how to check it and how to add a token that is connected to the Ethereum address of the wallet but not visible in Metamask.

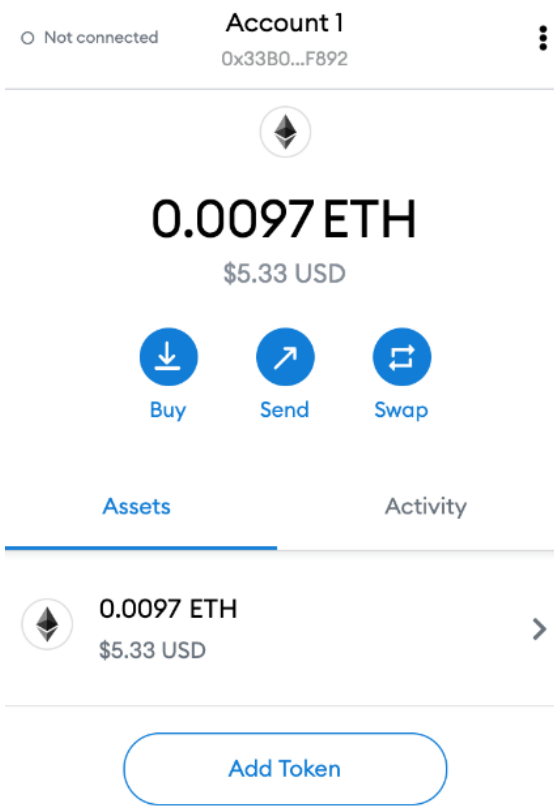
	Click on the Menu icon next to the Account (3 points) and click on "View on Etherscan" to be sure you did not miss any tokens to seize.
	Expand the view on the ERC-20 token holding and click on the name of the token.

	Copy the contract address of this token. You will find this at the right side of the page when you clicked on the token name (screenshot above). Continue as explained below.

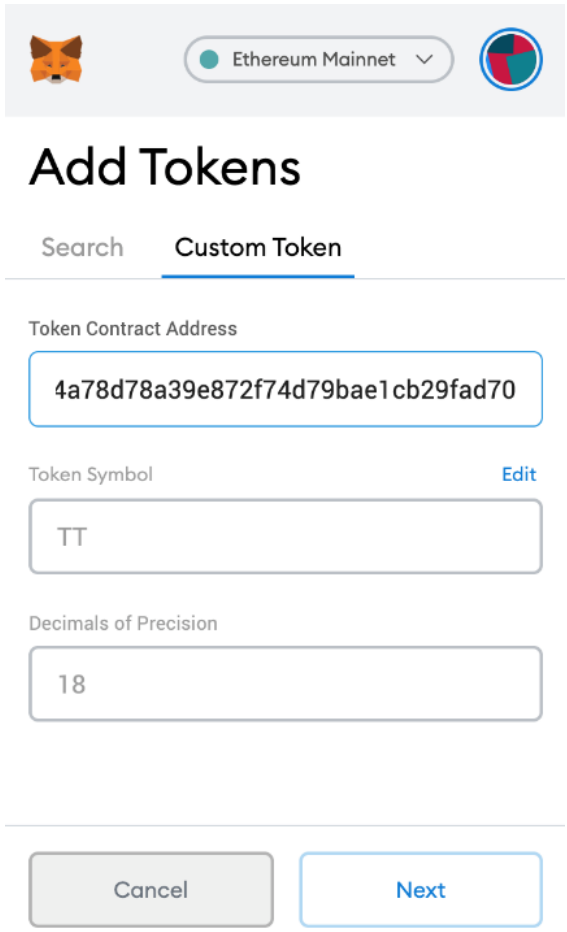
As you see, sometimes it will be necessary to add the "contract address" of a token to the wallet (in this case the TT token).

For your information: when adding a new token to track in the Metamask wallet, one of the form fields asks you for a 'Token Contract Address'. This refers to the address location of the actual token contract that manages the logic for the tokens. This does not refer to the address that holds your own personal tokens[28].

How to do this in Metamask:

	In the “Assets” tab, scroll down a bit and click on the blue button "Add Token".

[28] https://metamask.zendesk.com/hc/en-us/articles/360015488811-What-is-a-Token-Contract-Address



Click (tab) “Custom Token”.

Paste the contract address of the token you want to add.

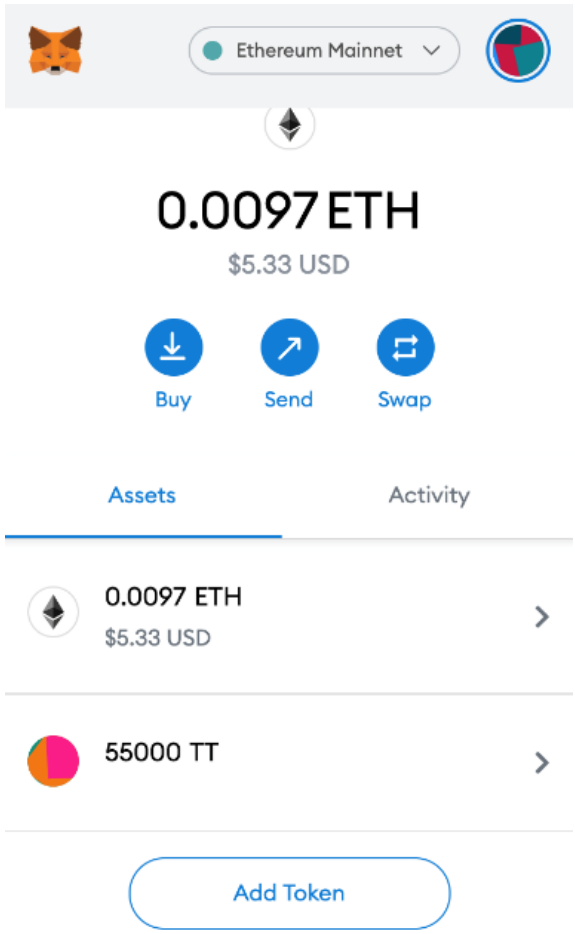
In this case, the contract address is: 0x54658e84a78d78a39e872f74d79bae1cb29fad70

Paste it in the field "Token Contract Address".

The rest of the form will be filled in automatically. Click "Next" and "Add tokens".

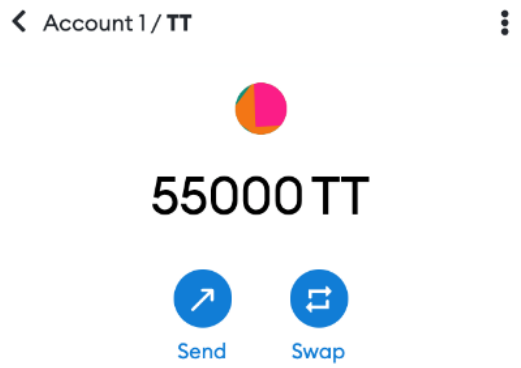
How to find token contract addresses is explained in the table above.

Click “Next”.

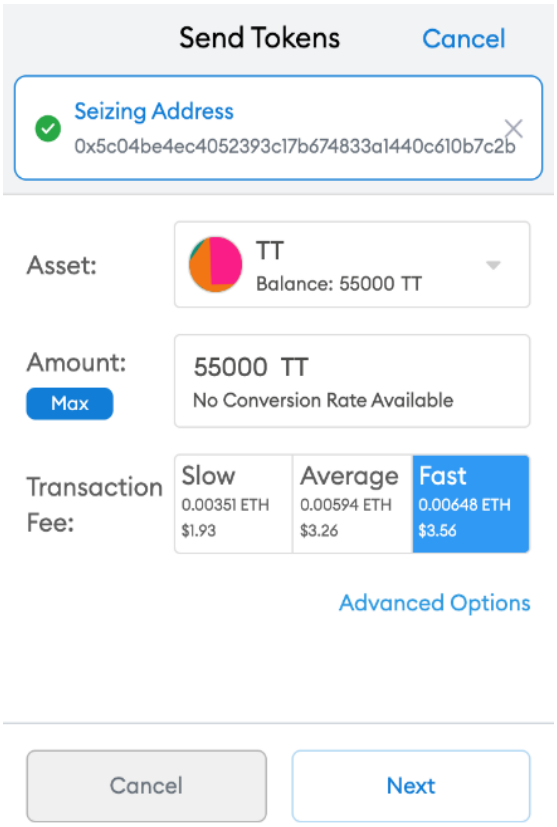
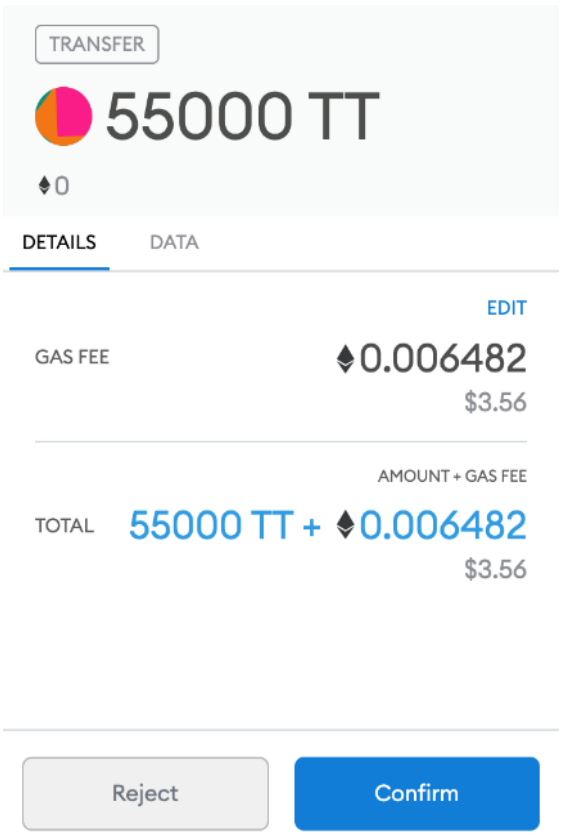


The token will now also be visible in Metamask.

Now, we can seize this token by clicking on it:



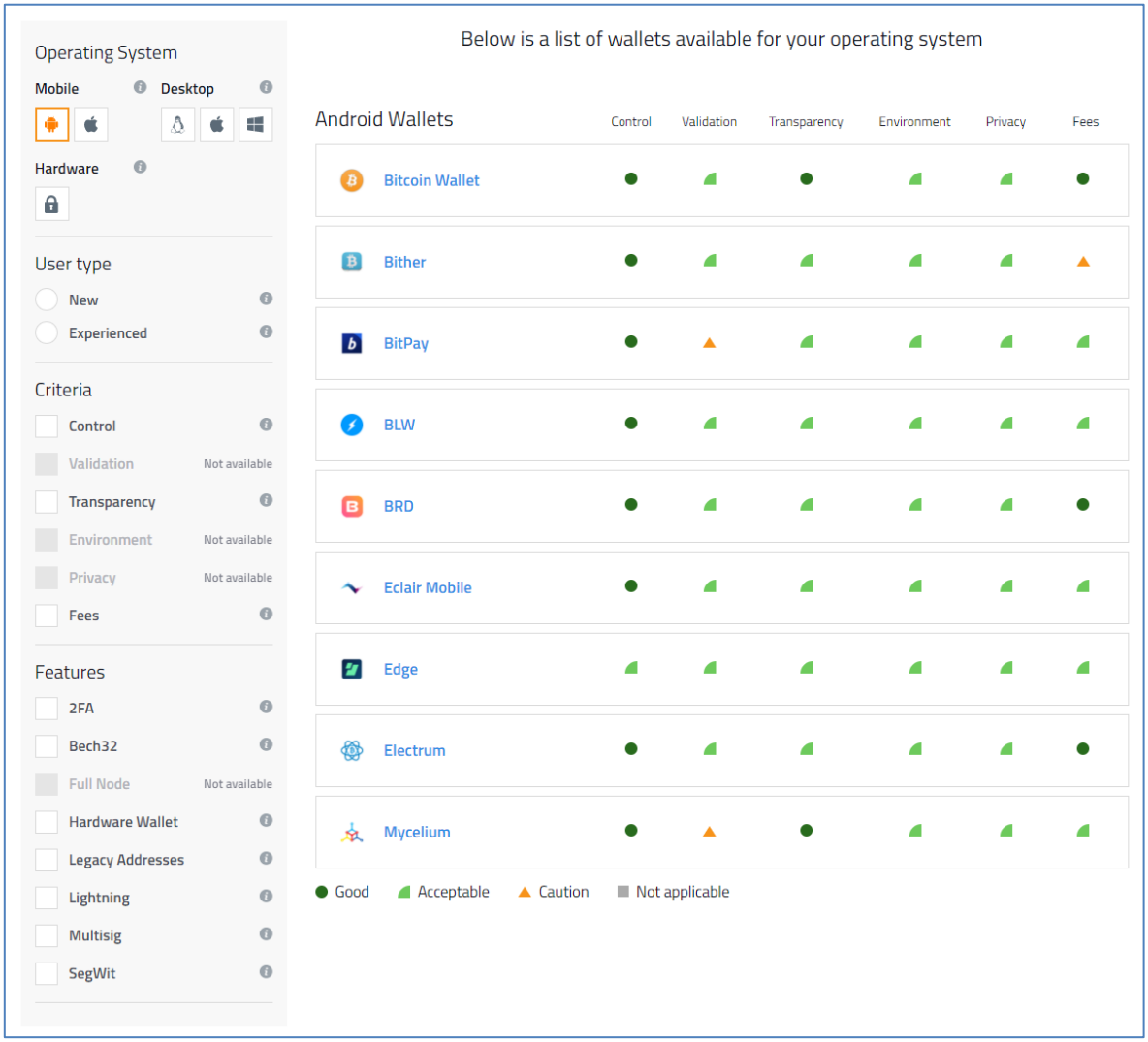
And next, click on the Send button.

	We are now in the Send Token screen. Paste the government-controlled seizing address. Click "Max" and choose "Fast" transaction. Click "Next".
	Now, you will see a confirmation screen. Click 'Confirm" to seize the tokens. If there are other tokens to be seized, do this first. It is recommended to continue by seizing the tokens with the highest balance. When all tokens are seized, send the Ether to that same government controlled Ethereum address.

3.4 Mobile Wallet

3.4.1 Introduction

There are many different types of wallets for iOS, Android devices and desktop environments. Since mobile payments and the ease of use makes it widely available to the large public, you do not need to be a cryptocurrency expert to be able to scan QR codes to spend and receive cryptocurrencies. From Bitcoin.org[29] you can find a multitude of different apps for different platforms. In this chapter we will introduce a few that are widely used and popular. Once you have access to the suspects computer or mobile device, noticing one of these logos is a definite clue of cryptocurrency use.



3.4.2 Best practices and guidelines

Seizing from mobile wallets can be a bit tricky. If you do not have a QR code to the government wallet, you need to type in the address manually which, considering you're typing in a mobile device, can be sensitive in making mistakes.

However, since creating a QR code is quite easy, it is recommended to have one of these converters installed on a secure computer and when going to the arrest or house search you should have the QR

[29] https://bitcoin.org/en/choose-your-wallet

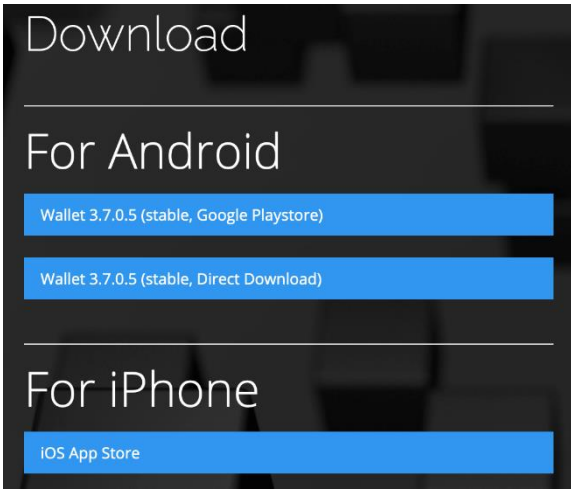
code and the text string ready for seizure. Of course, situations might arise when you run into completely new cryptocurrencies that you have never heard of but considering how time sensitive cryptocurrency seizures and confiscation is, you might need to have a blank mobile device with a multicurrency wallet ready or even be prepared to use a swap service if authorized by the person in charge.

3.4.3 MyCelium

- Uses 12-word seed phrase (BIP39 compatible)
- Uses PIN-code: optional for opening the wallet and for sending
- Can store bitcoins (BTC) and ether (ETH) (+ tokens)

MyCelium (next to Jaxx Liberty and Exodus) is one of the most popular crypto wallets and just like many other, MyCelium also provides in-app coin swapping which has become quite popular amongst criminals to obfuscate the source of the funds.

Installing MyCelium can be done on an Android phone without registering to Google services, which might come handy as anonymity is important for everyone. Direct download of MyCelium app for Android and iOS can be done from https://wallet.mycelium.com/contact.html.

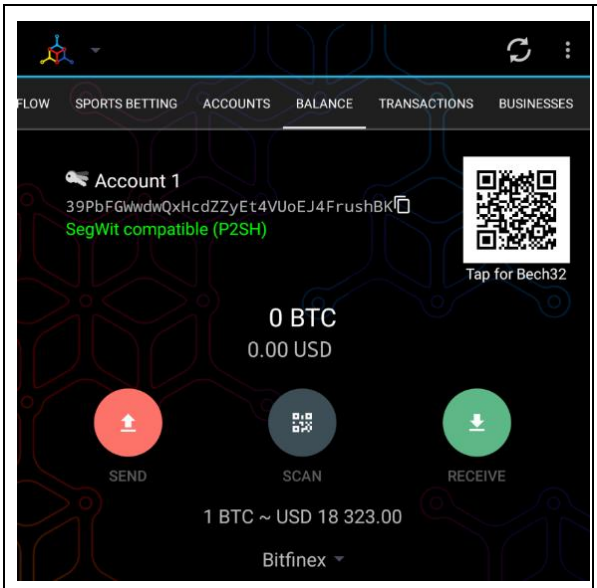


Once downloaded, the installation process is quite straight forward. First start the app file and in this example, it is an Android version. Next, it will ask permission for installing the .apk from unknown source which you must grant.

This wallet can be routed over Tor and is compatible with Ledger and Trezor hardware devices. For more info, we refer to the following web pages:

https://support.ledger.com/hc/en-us/articles/115005199449-Set-up-Mycelium-on-Android
https://wiki.trezor.io/Apps:Mycelium

Seizing in MyCelium (no PIN's used or PIN is known by the investigator)

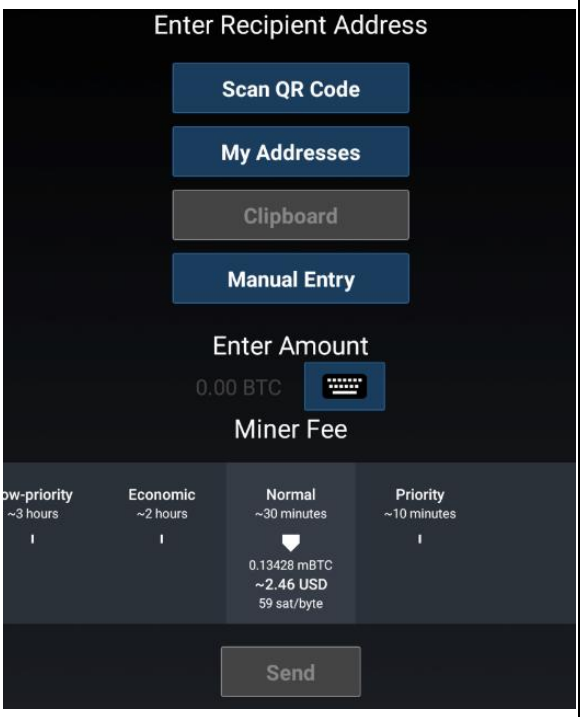


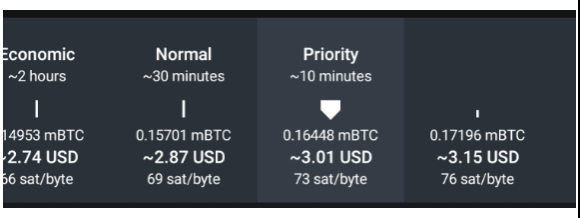
In the Balance screen (= home screen) we can see how much funds are in the wallet and what type of funds (Bitcoin, Ethereum or – tokens).

What is mentioned below in this screenshot (Bitfinex) is not relevant for us. It means that this user chooses the Bitfinex API to get the current Bitcoin price.

This Bitcoin account (address starts with 39PbF) has no bitcoins. No funds could be seized here.

If there were any funds here, one could simply click on the red "Send" button.





After clicking on "Send", a new screen pops up.

The seizing address (government-controlled) could be entered here by scanning a QR-code or by entering it manually. Also remember the safeguards of checking the address where you are sending the crypto currencies to, the four-eyes rule.

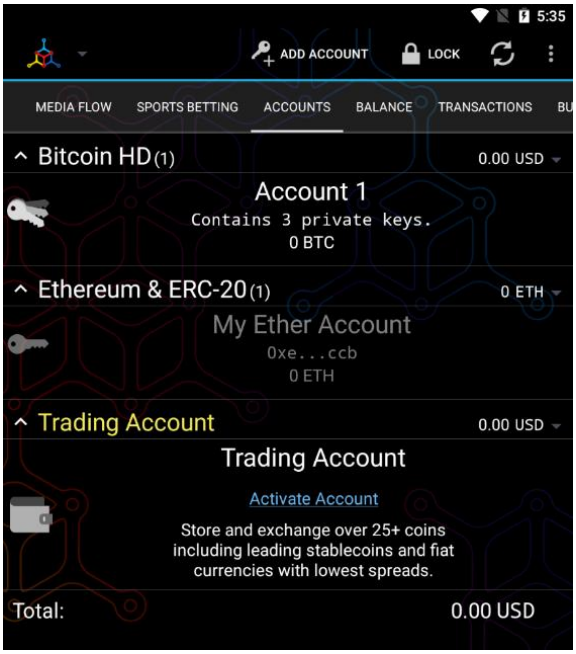
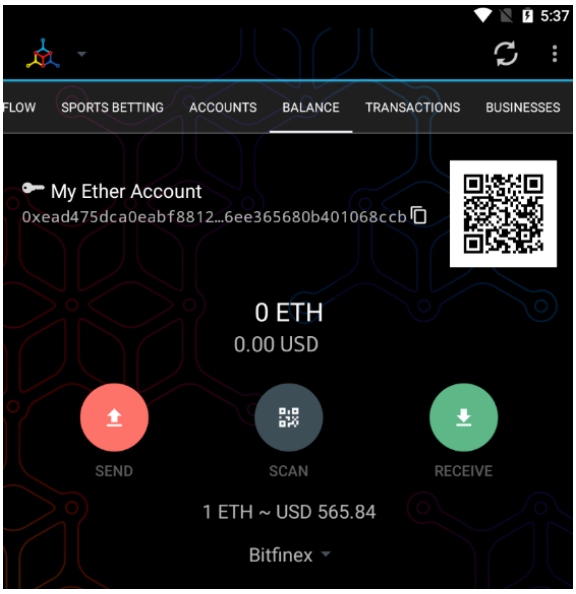
A manual entry should be avoided because mistakes are easily made when typing in bitcoin addresses. Try a copy-paste instead and again double and triple check the address since there are malware that might alter the address.

Next, enter the total amount or just set it to "max" of bitcoins and choose a transaction fee. Note that you need to do this process to every account found on the app separately, start with the ones with largest balance.

The transaction cost is mentioned below and the faster the transaction need to be confirmed by the Bitcoin network, the more the fee will be.

The higher the fee, the faster the transaction is confirmed in the blockchain, the less probability, eventual accomplices can overrule it with a copy of the wallet on their device.

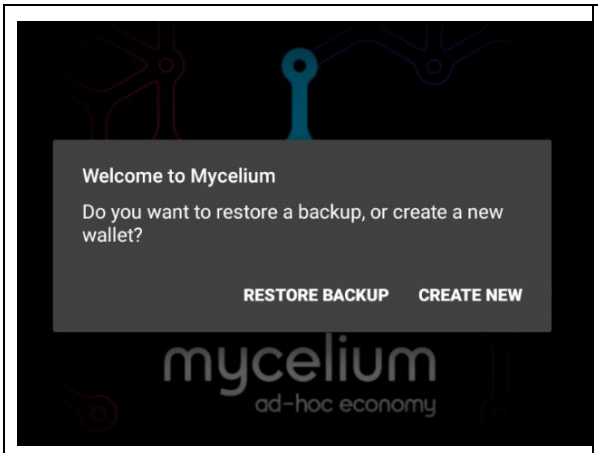
Finally, click "Send" to seize the bitcoins.

	Click on "Accounts" to see if there are any other cryptocurrencies to be seized. For example, this screenshot also shows the presence of an Ethereum account. Click on "Ethereum & ERC-20" and click on "Balance".
	We are now in the Ethereum account of MyCelium. Follow the same procedure as explained above. If there are any ERC-20 tokens (e.g., USDC, DAI, BAT, …) seize them first. Use the same Ethereum seizing address for Ethereum (ETH) and tokens.

Seed found

MyCelium uses a BIP39 compatible 12-word mnemonic phrase that is compatible with other BIP39 compatible wallets[30].

[30] Refer to https://www.blockplate.com/blogs/blockplate/list-of-bip39-wallets-mnemonic-seed for a list of compatible wallets.

	When a 12-word mnemonic phrase was found, you can use any BIP39 compatible wallet to restore the funds. This screenshot shows the Restore screen of MyCelium After typing in these 12 words, you will arrive in the Balance screen as explained above.

3.4.4 Jaxx Liberty

- Uses a 12-word mnemonic (seed phrase), but no password by default.
- Supports swaps with Simplex, ShapeShift and Changelly.
- Can be paired with other devices on iOS, iPadOS or Android.

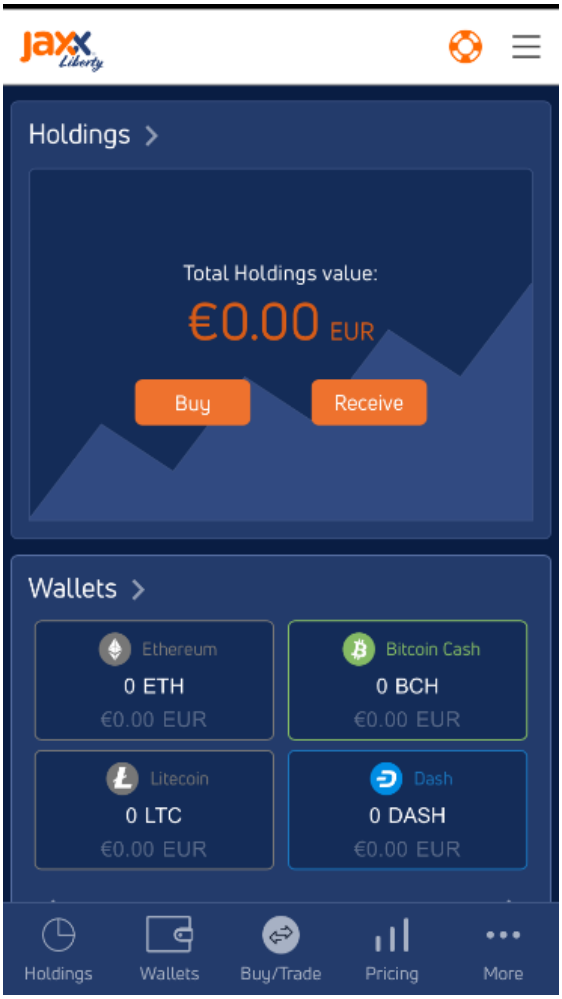
Attention:

When seizing Bitcoin from this wallet: do not use a native SegWit (Bech32) Bitcoin address. A Bech32 address starts with bc1. Jaxx Liberty (Version 2.4.6 #289) cannot send to these addresses.

Solution: use a Bitcoin seizing address that starts with 1 or 3!

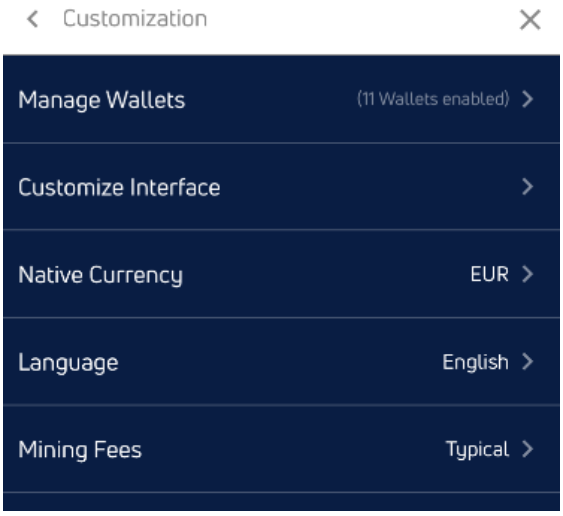
Option 1: password found, or no password used

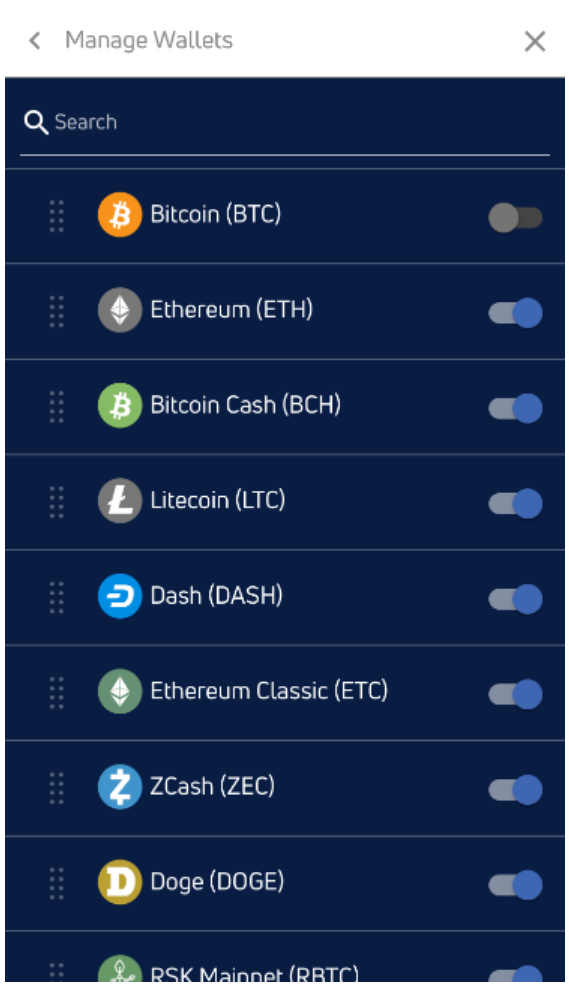
Pro Tip: users can activate and deactivate the different cryptocurrency wallets. For instance, if a user wants to hide for instance his Bitcoin holdings in Jaxx, he can deactivate the wallet so the "Total Holdings value" will show 0 EUR!



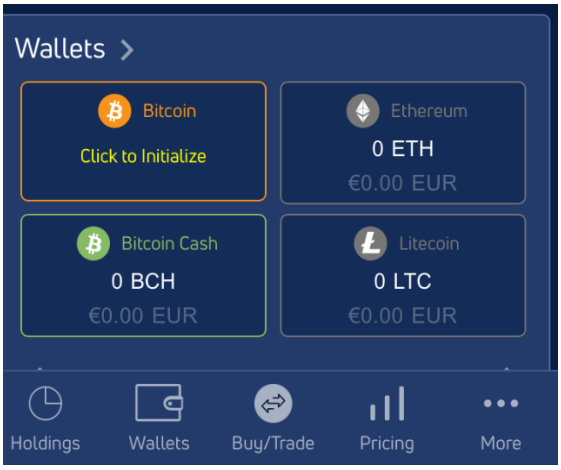
This is a possible scenario: the wallet seems empty so let us first check if there are any deactivated wallets.

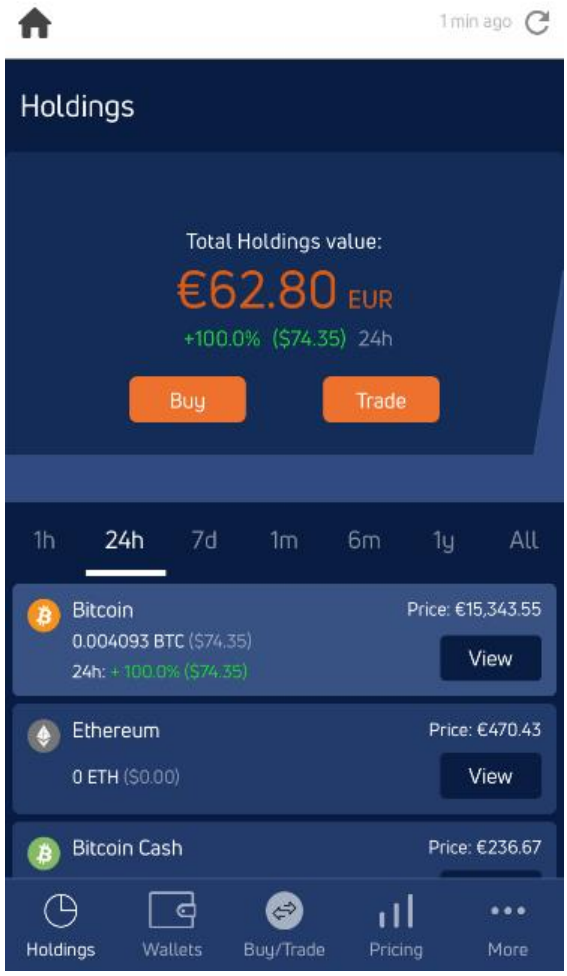
To find it out, click on the round icon on the top right and click on "Manage Wallets".





The screenshot on the left indicates that the Bitcoin wallet is deactivated. Click the switch to activate this wallet. Then, go back to the Home screen and "Click to Initialize".

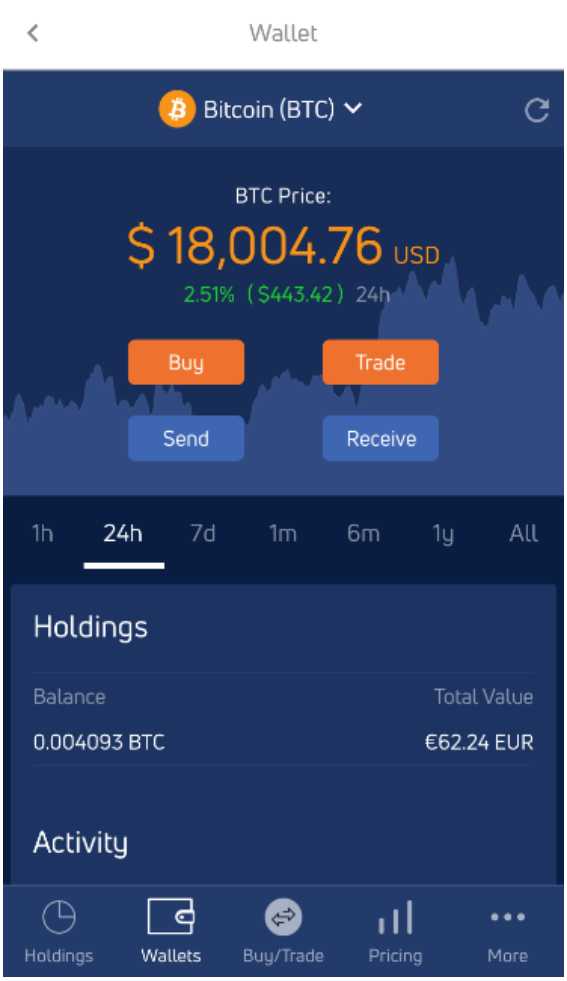




Only the Bitcoin wallet has funds.

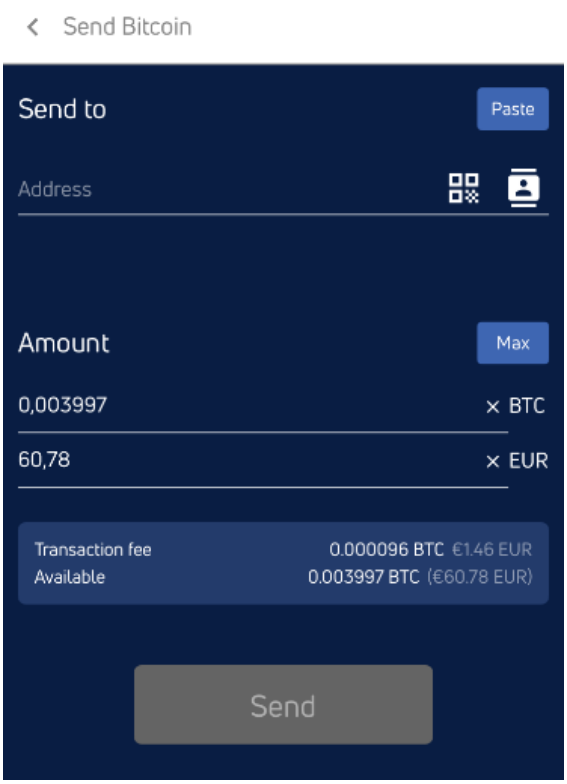
To seize the funds, click on Bitcoin and again (in the Wallets screen) on Bitcoin.

The seizing itself can start from here.



In the Bitcoin wallet of Jaxx Liberty, the total BTC holdings are mentioned (0.004093 BTC).

Click Send to seize these funds.

	In Address, paste the Bitcoin seizing address. Click "Max" to send the full amount. The transaction fee will be mentioned below. Click "Send" to seize. If you have found other cryptocurrencies in this wallet. Follow the same procedure.

Option 2: seed was found

A 12-word seed phrase can be used with many different wallets. If the suspect has Jaxx on his mobile, chances are that this is the seed for Jaxx. Try to use a seed with different wallets (or a tool) since not all wallets use the same derivation paths. Sometimes they will show a zero value when there should be a positive value just because not all the wallets follow strictly the same derivation algorithm or BIP39 standards.

3.5 Hardware Wallet

3.5.1 Introduction

Hardware wallets have come very popular in the past years, they are considered to be the best and safest storage for many different cryptocurrencies. They are considered to provide better safekeeping than a paper wallet described at the end of the document.

For some agencies, the best practice is to use paper wallets, put in a tamperproof evidence bag, but some law enforcement agencies use hardware wallets to safekeep their confiscated assets. This might be ok when a limited amount of people has access to the device. However, every time the PIN code is entered, there is a potential risk of someone getting unauthorized access to it and eventually stealing the virtual currencies found on the wallet.

These wallets also have the typical seed word practices which might be a point of compromise. The seed word process and how to set up a Ledger wallet is described in the ledger wallet setup and confiscation process.

3.5.2 Best practices and guidelines

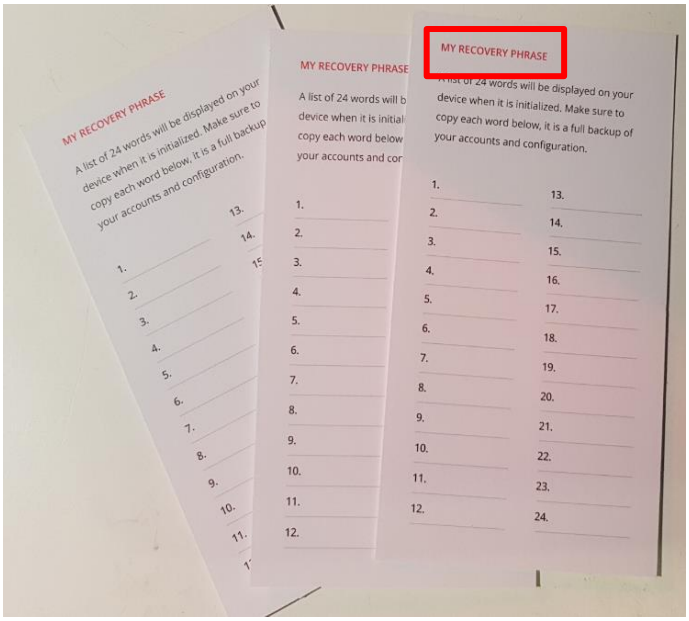
3.5.2.1 Ledger wallet

Recently, it has been observed that many criminals have started to use hardware wallets since they are more secure, able to store multiple currencies, and very difficult to open or brute force without the help of the suspect.

A Ledger device is PIN code protected and after 3 wrong PIN code attempts it blanks/erases itself, making it impossible to restore any of the virtual currency data without the seed words. It is recommended to have a few hardware wallets (Ledger, Trezor, KeepKey, etc.) in hand since some of them actually return different sets of private keys when restoring them and also they are considered quite safe. Also, in trainings it is good to learn how to install and restore these types of wallets.

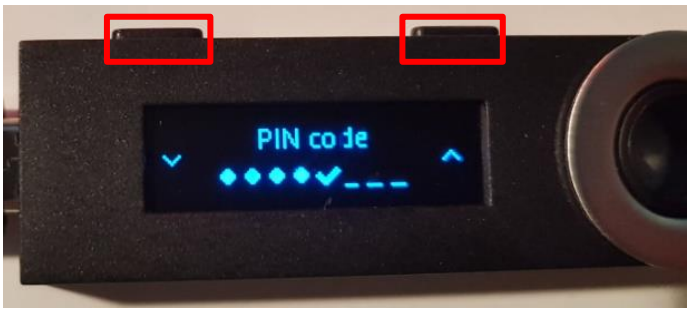
We will now investigate a clean installation of a "Ledger Nano S" wallet from unboxing to transferring bitcoins to it and restoring it.

	A new Ledger Nano S, in packaging, is shown in the left picture. The device itself looks like a normal USB device and it comes with a micro-USB cable with the ledger logo on the cable (this is also a clue of cryptocurrency use, or even the box itself), as shown in the screenshot. Most importantly for an investigator we have the sheet which says Recovery sheet or MY RECOVERY PHRASE. These are also displayed and highlighted in the pictures on the left.

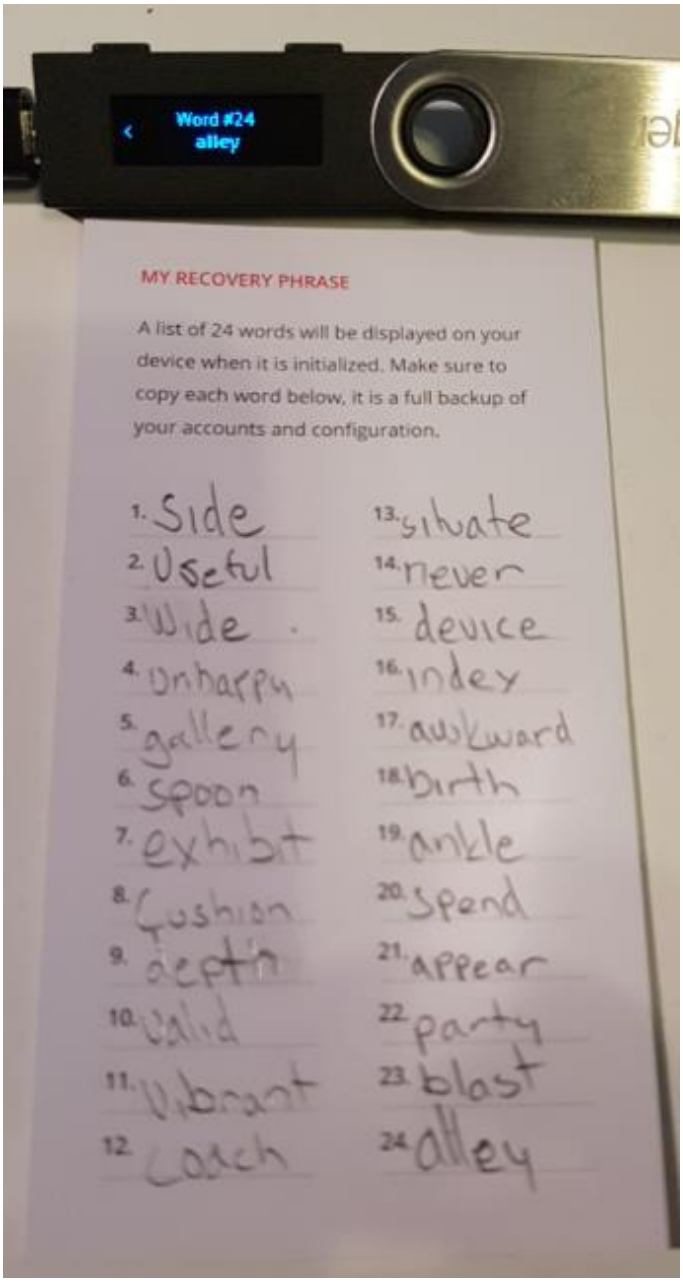

MY RECOVERY PHRASE
A list of 24 words will be displayed on your device when it is initialized. Make sure to copy each word below, it is a full backup of your accounts and configuration.

To install a new wallet, follow the following steps. These wallets can then be used as seizure for government-controlled wallets. By default, to confirm an action you need to press both buttons on the top to confirm your selection.

Plug in the device with the micro-USB cable to your computer USB, the device should immediately come to live and asks to press both buttons to begin (the two

	buttons are located on the top of the device).
	Select the button at the right and configure as a new device. Select a new PIN code.
	Confirm the PIN code by pressing both buttons on the ledger device.
	Now, we will get the 24 seed word that we write down on the given sheet.
	Word 1.

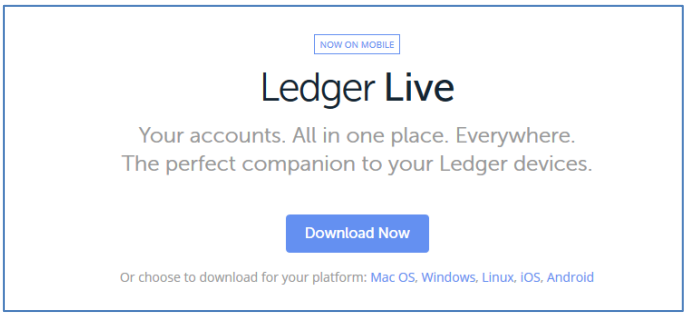
Word 2.

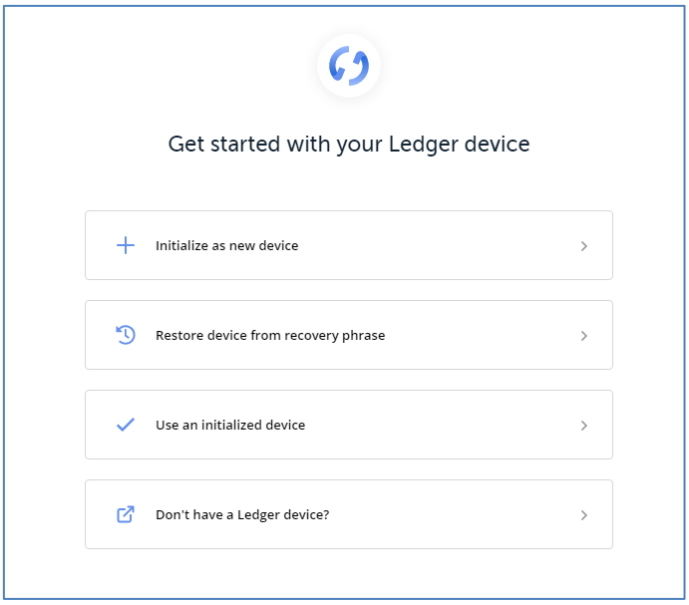


Word 24 and the full seed word list as depicted left.

Now, we must confirm all the 24 words that we have written down, and essentially, we would be able to restore the same wallet to any compatible BIP39/BIP44 device.

After receiving all the seed words and confirming them, the device is ready to be used.

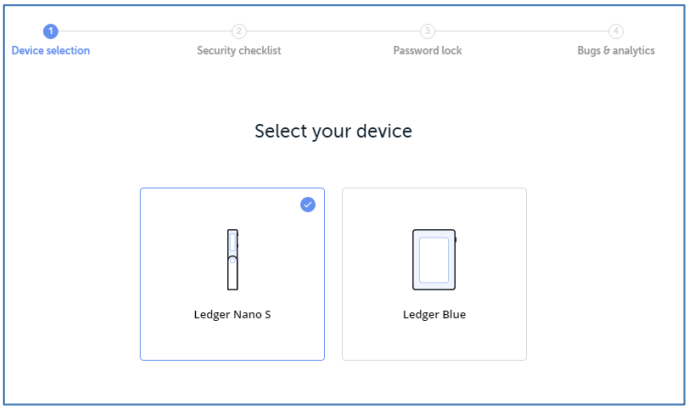

NOW ON MOBILE
Ledger Live
Your accounts. All in one place. Everywhere.
The perfect companion to your Ledger devices.
Download Now
Or choose to download for your platform: Mac OS, Windows, Linux, iOS, Android


Get started with your Ledger device
Initialize as new device
Restore device from recovery phrase
Use an initialized device
Don't have a Ledger device?

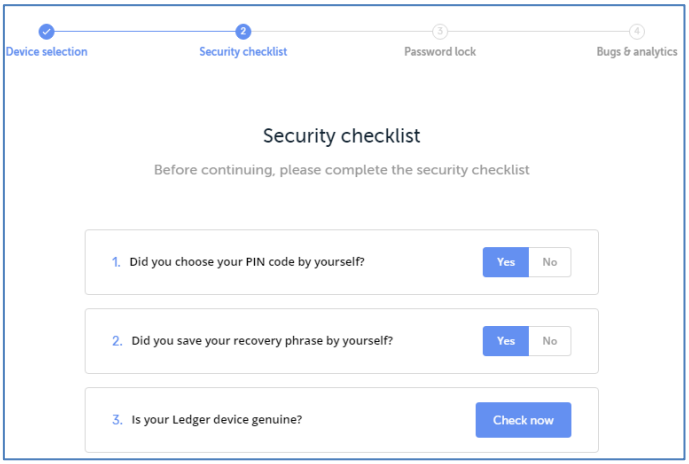
The next step is to install the virtual currency applications to the device that we want to use.

Installing Bitcoin application on Ledger Nano S. Navigate to https://www.ledger.com/pages/ledger-live and download and install the Ledger Live application for your platform.

As in the previous example we already did the initialization process, we can select use an initialized device. Note that the same process we did manually on the device can also be done through the Live app.



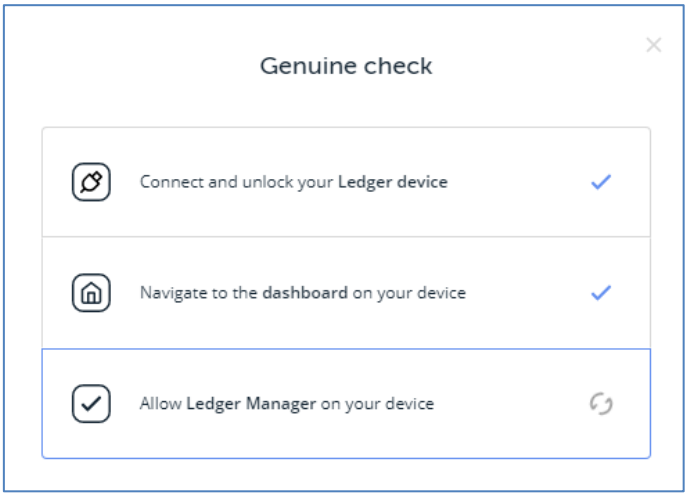
There will be a few questions since there has been some used and counterfeit devices sold on the internet and people who did not initialize and install the device themselves have been stolen their virtual currencies.



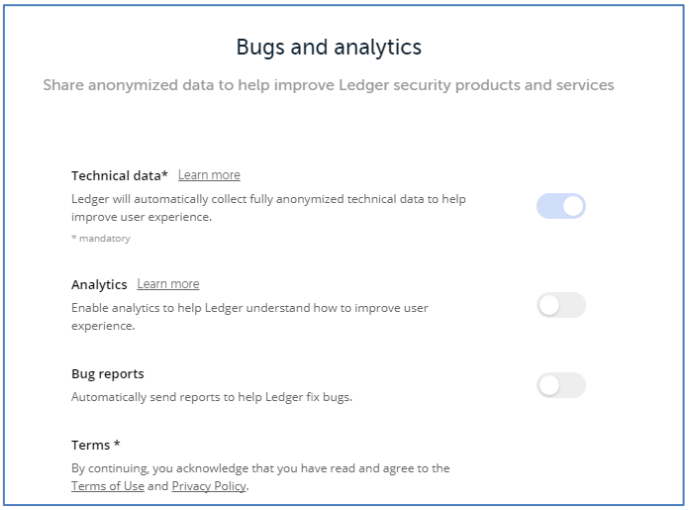
Select "Did you actually set it up yourself?"

Select "Did you save your recovery phrase by yourself?"

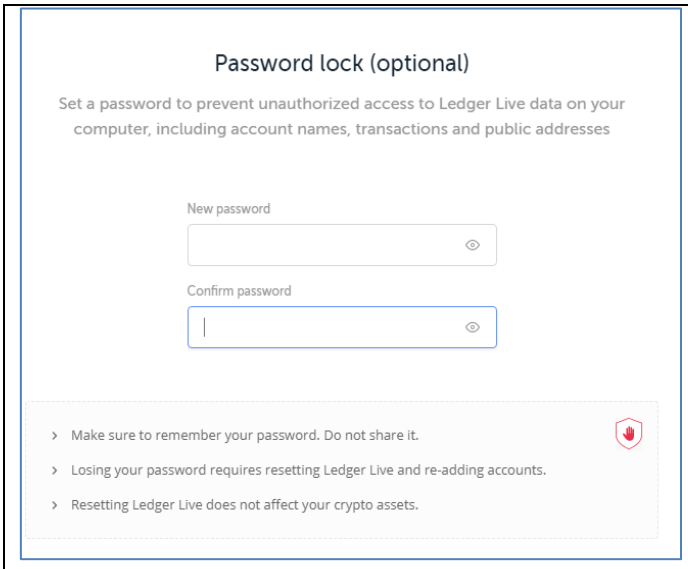
Click "Check now" to go to the "Genuine check" of the device.


Genuine check
Connect and unlock your Ledger device
Navigate to the dashboard on your device
Allow Ledger Manager on your device

Click the right button on the device to "Allow Ledger Manager on your device".


Bugs and analytics
Share anonymized data to help improve Ledger security products and services
Technical data* Learn more
Ledger will automatically collect fully anonymized technical data to help improve user experience.
* mandatory
Analytics Learn more
Enable analytics to help Ledger understand how to improve user experience.
Bug reports
Automatically send reports to help Ledger fix bugs.
Terms *
By continuing, you acknowledge that you have read and agree to the Terms of Use and Privacy Policy.

Permissions to send data and analytics to the Ledger company (disable).

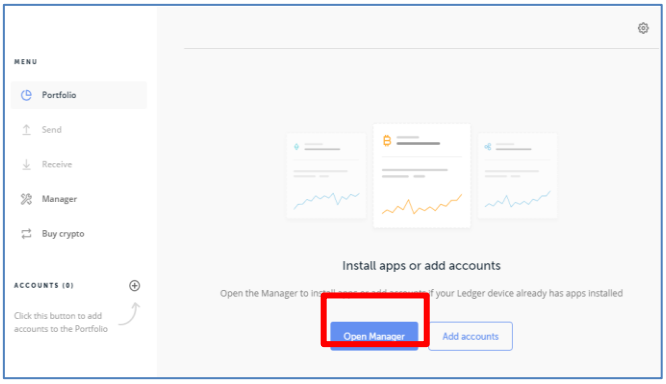

Password lock (optional)
Set a password to prevent unauthorized access to Ledger Live data on your computer, including account names, transactions and public addresses
New password
Confirm password
Make sure to remember your password. Do not share it.
Losing your password requires resetting Ledger Live and re-adding accounts.
Resetting Ledger Live does not affect your crypto assets.

And finally generate a secure password for your Ledger Live app.

Note that with the PIN code you can access the device from another computer though a clean installation of Ledger Live and a different password.

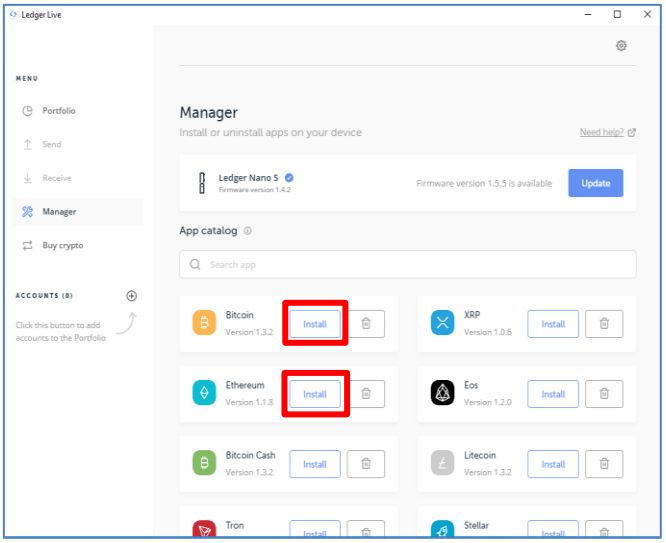
This means that the ledger Live password is saved locally.

Also, if you have the seed words you can restore the wallet to any computer.



After installing the wallet, we can now create (for example) a government-controlled seizure wallet to the Ledger.

In the main window, select ”Open Manager”.

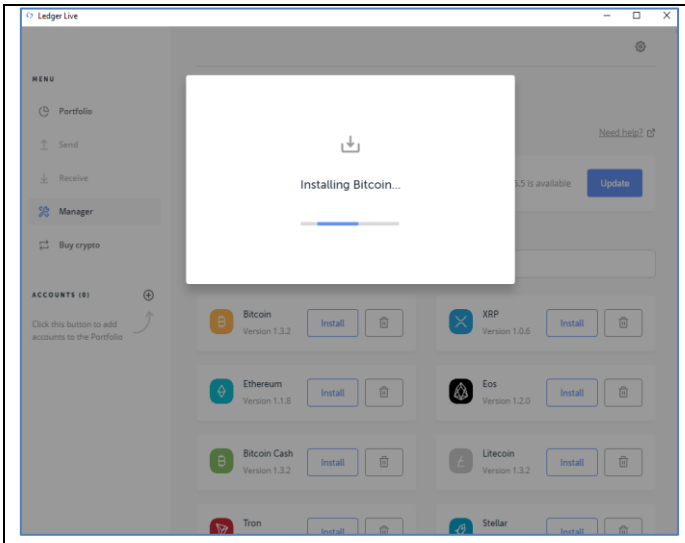


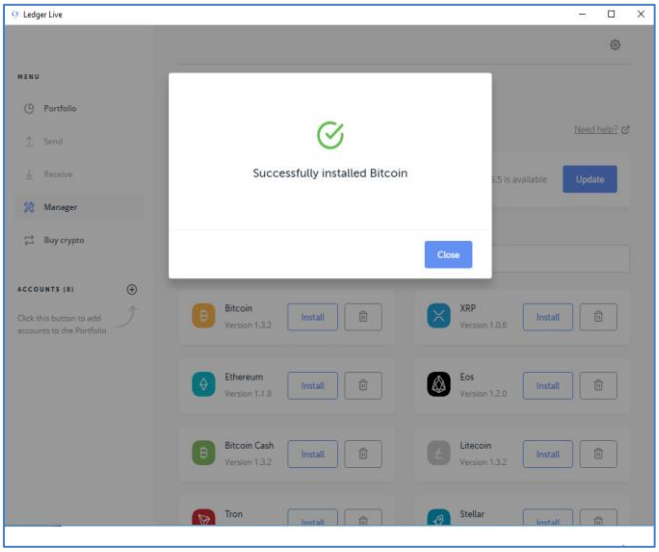
To install the Bitcoin app, open the “manager” and select “install” on the Bitcoin box.

For Ethereum, select “install” next to the Ethereum app. Both are highlighted (red box) in the picture.

It will take a few minutes to install the Bitcoin wallet into the Ledger Live app and into the Ledger device.

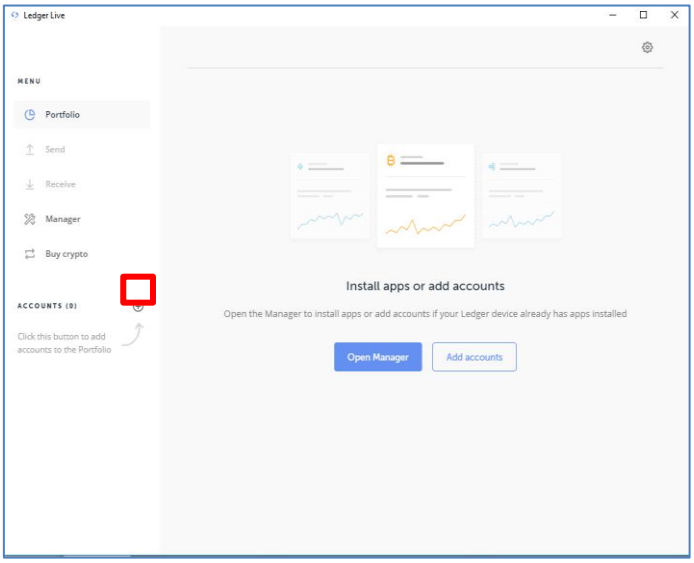
You must also confirm the Ledger Manager’s access on the device by pressing both buttons on top of the device itself (as mentioned above).





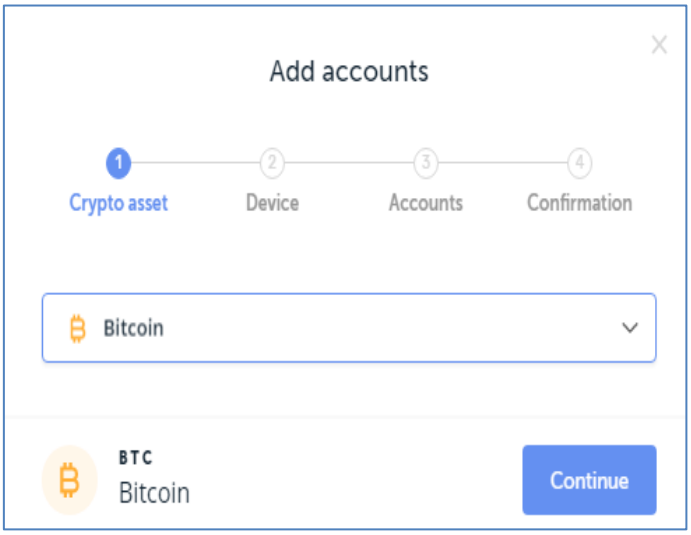
After the Ledger Live shows that the installation has been successful, you should also have the Bitcoin logo on the Ledger device.

The Bitcoin app should be displayed on the Ledger device upon successful installation.

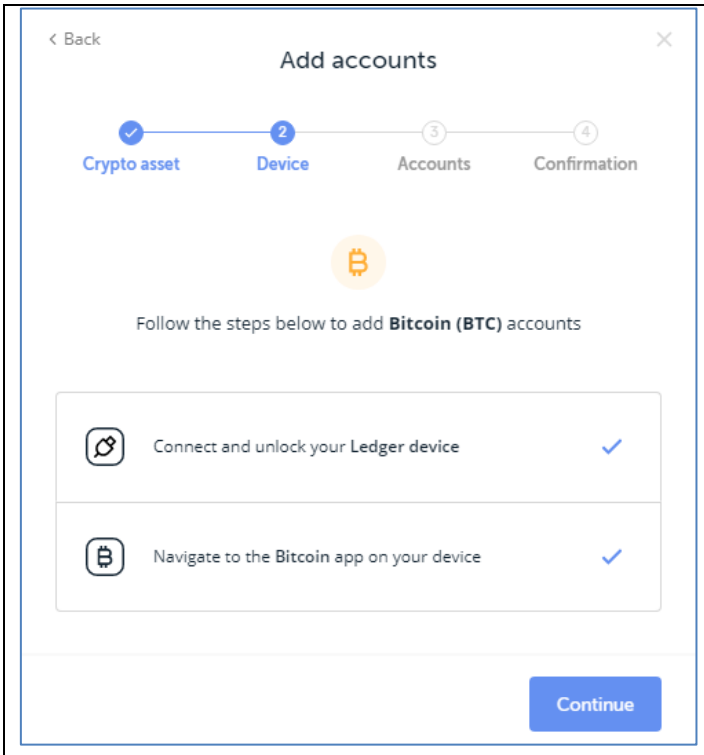


Adding a government-controlled account is a very straight forward process. On the Ledger device there can be stored many different cryptocurrencies and tokens and since for smaller units might be a handy and easy solution for most cases.

Select the plus sign after "Accounts" (+) highlighted in the picture.

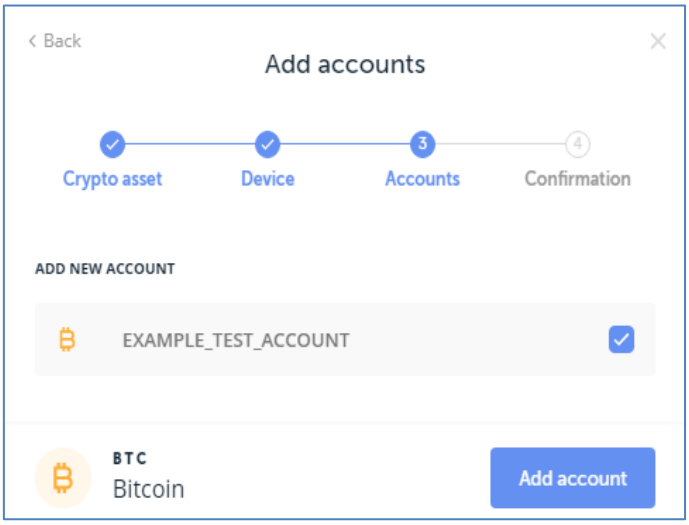


Select "add account" and the virtual currency type.



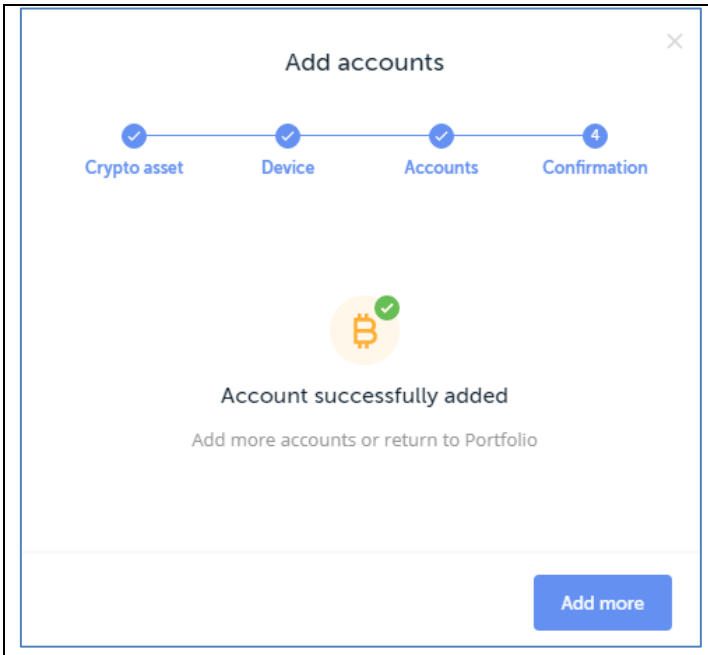
Connect and unlock the Ledger device itself.

Select the Bitcoin app from it (not in picture).



Give the account the desired name.

E.g., a case name (in the example it is called "Example_test_account").



Once you have given it a name, it is ready to be used and sent bitcoins to.

You can follow the same process for different currencies like Litecoin, Ethereum etc.

Restoring and seizing of an Ethereum ERC-20 token will be addressed later in this document.

Restoring a Ledger device with the seed phrase.

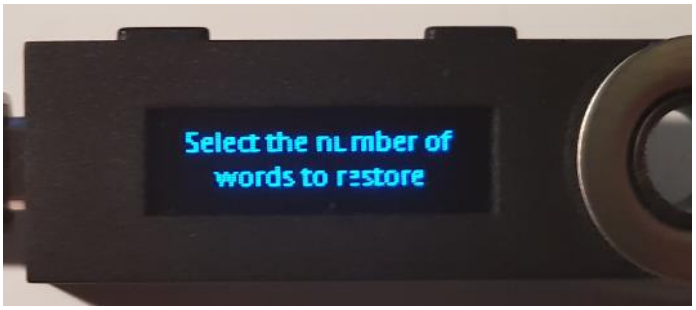
Restoring a Ledger device from seed words can be done directly from the device. It is quite much alike the installation process and the device will guide you through the process.

This is a very important process to learn and to practice.

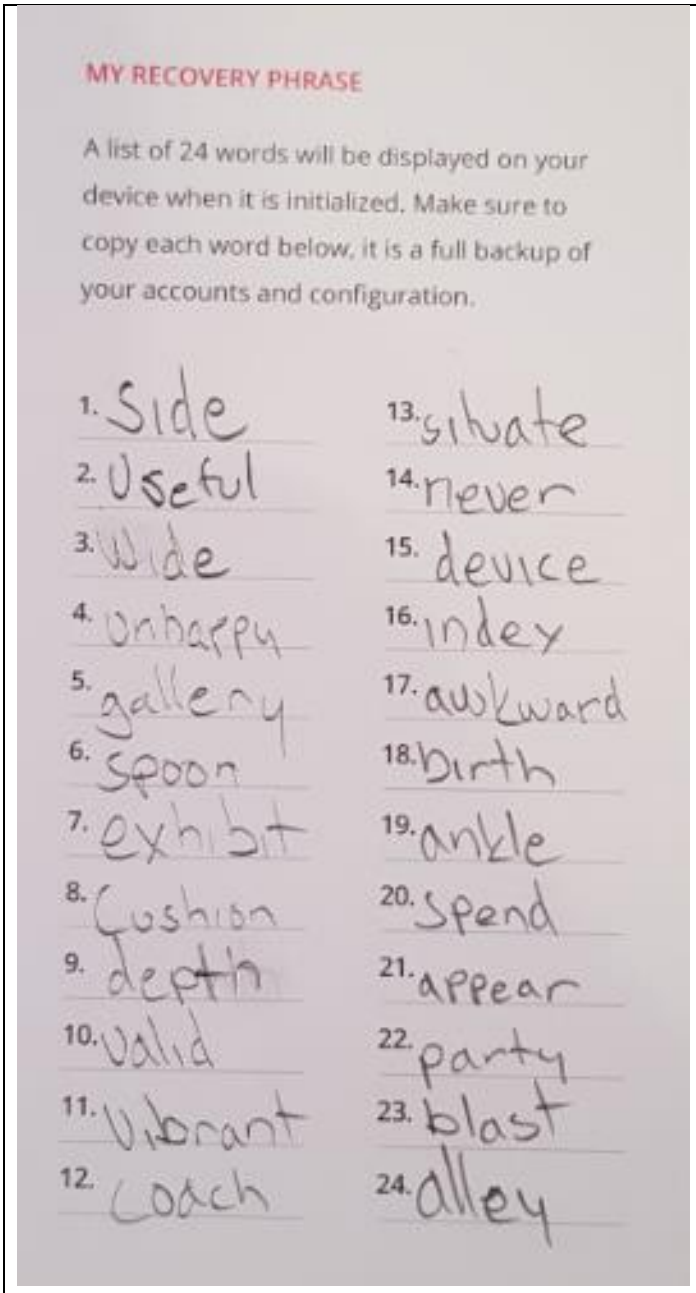
It will increase your self-confidence at the confiscation scene.

This results in the fact that you will be able to do a seizing quickly and before someone else can access the wallet.

In general, wallets can be used in another location at the same time by using the seed phrase.

	Select "X" by clicking the left button on top of the device (do not configure as new device!).
	Select "Restore configuration?".
	Choose a new PIN code. This code does not have anything to do with the old PIN code or the suspect's possible PIN code.
	Enter the recovery phrase (seed) from the seed words.
	

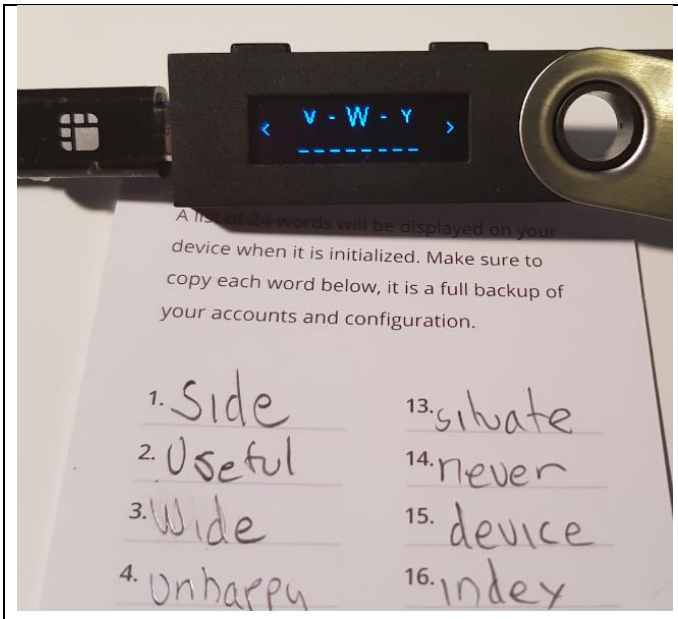
Since this wallet also supports other wordlists (lengths) you can restore any 12 – 18 – 24 seed word list into it.



Restoration starts with the first word from the wordlist that we have found at our suspect's premises.

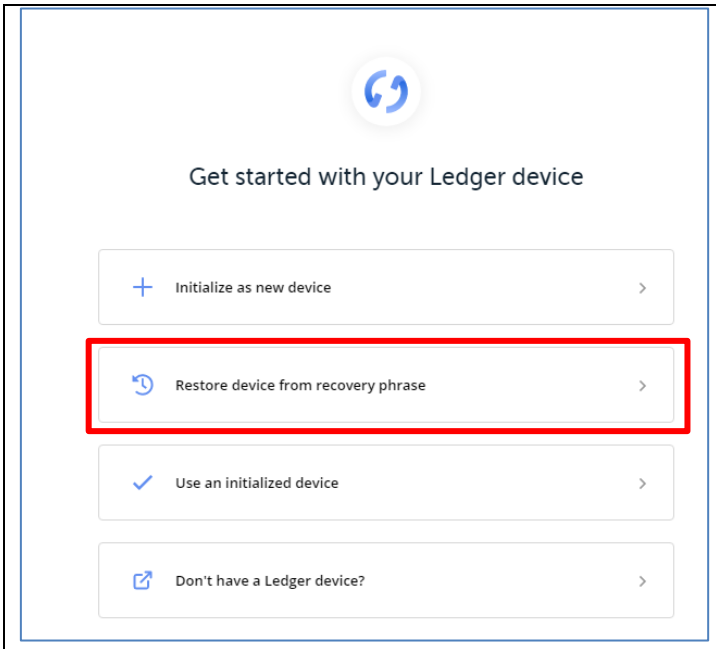
We use our recovery phrase.

Enter the first letter of the first word.


v - W - Y
device when it is initialized. Make sure to
copy each word below, it is a full backup of
your accounts and configuration.
1. Side
2. Useful
3. Wide
4. Unhappy
13. situate
14. never
15. device
16. index

Processing...

Your device
is now ready


Get started with your Ledger device
Initialize as new device
Restore device from recovery phrase
Use an initialized device
Don't have a Ledger device?

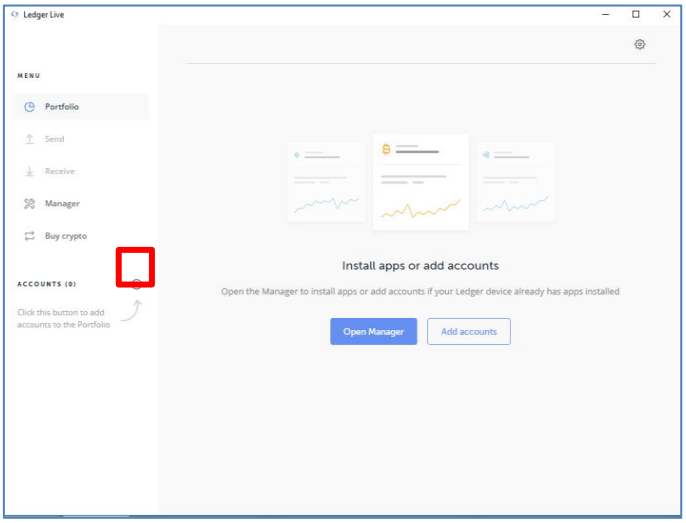
After the 24th word, the device will process the given seed words and return you an exact copy of the wallet.

Now we must install the Ledger Live application and repeat the process of installing the Bitcoin app.

Note that if you need to find out other virtual currencies you must install all the apps one by one.

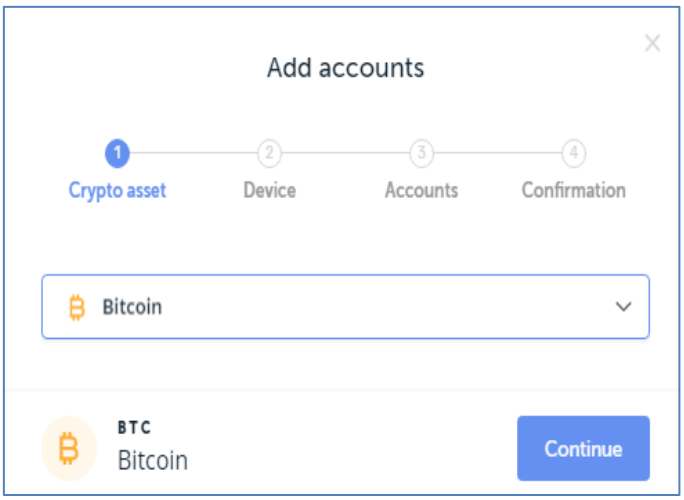
Also note that you cannot install all the cryptocurrency apps at once since the memory bank on these devices is too small.

After installing Ledger Live, we will select restore the device from recovery phrase (it will give a short instruction to the same steps as described before).

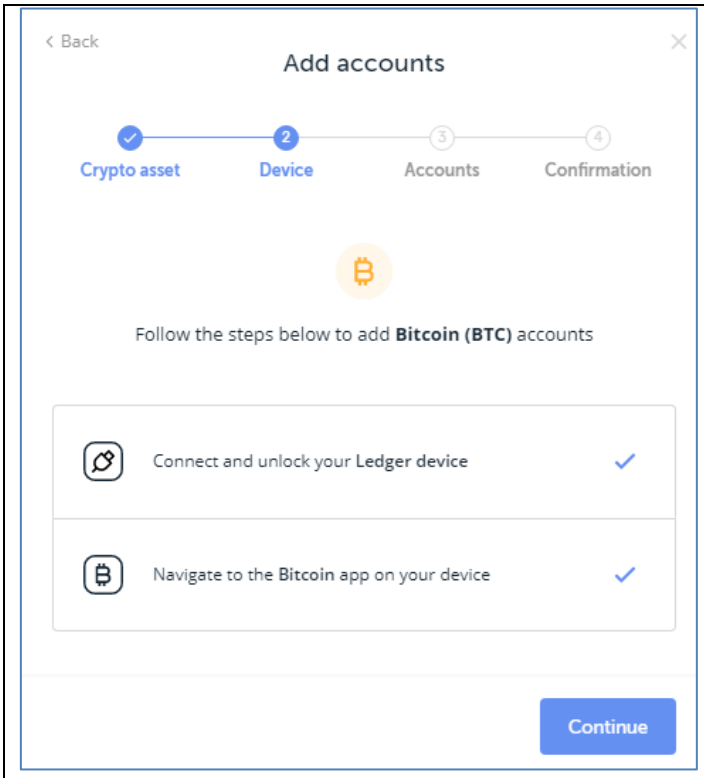


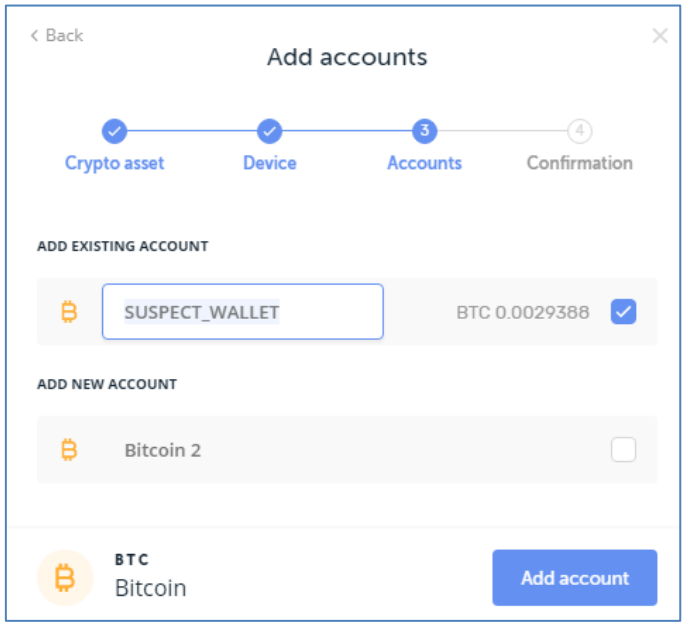
After installing the Bitcoin app we need to open the manager and install the Bitcoin app to the ledger device, just like in the steps described earlier to install an app.

Install new account by pressing the (+) button.

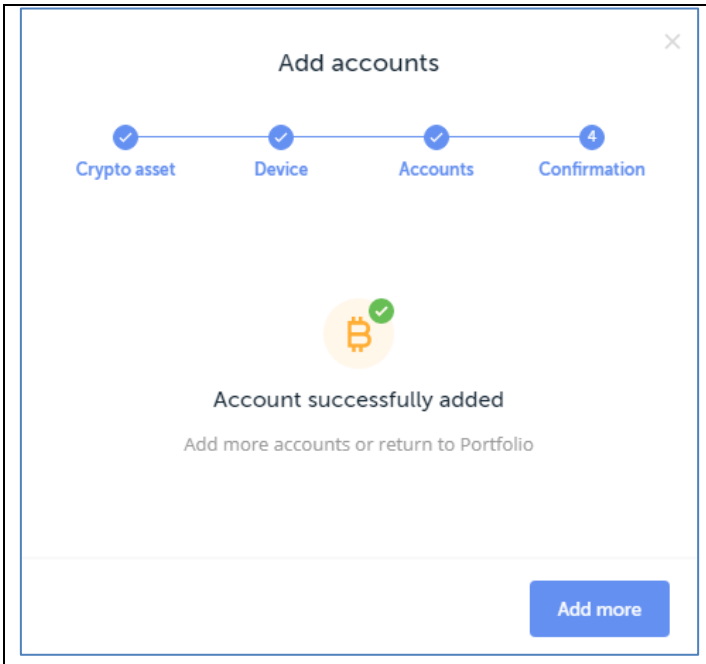


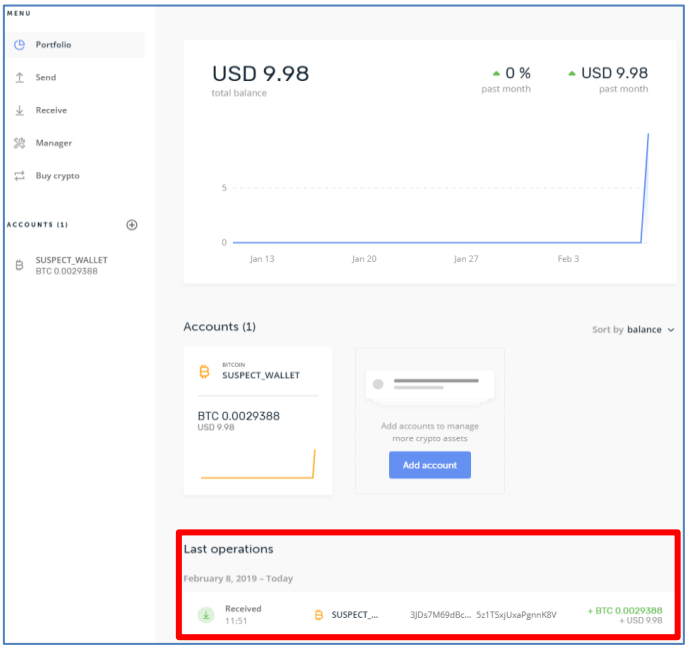
Select the asset you want to add and connect your ledger and unlock it.





After synchronization, the suspect's Bitcoin account should appear if everything has been done correctly and the given seed word was the actual that was used. You can name the account anyway you like, here named "SUSPECT_WALLET".





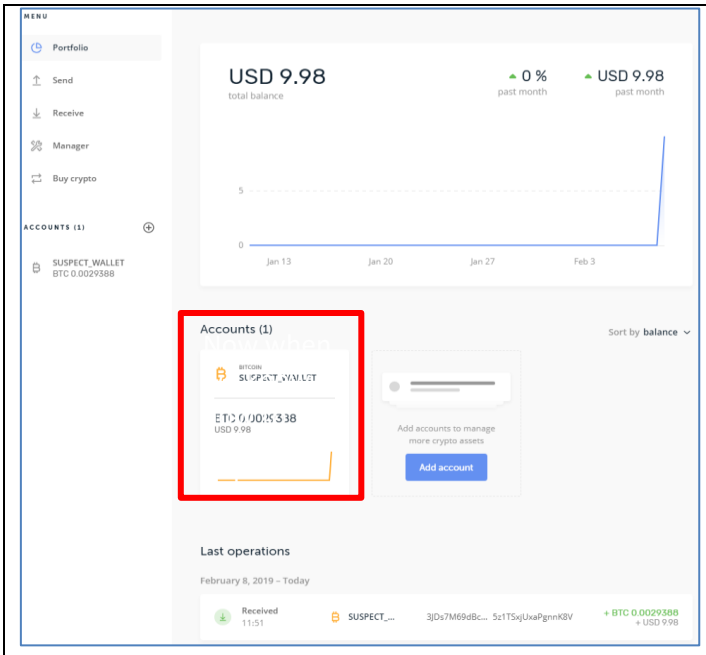
After the installation and synchronization of Bitcoin we notice that we have access to the funds of Bitcoin account 1, derivation path `0.

It must be noted for all the derivation paths you need to add the accounts manually one by one. Derivation paths were discussed later in this document.

Even in the case that all the funds were sent out, we would still have the history from where we can extract the Bitcoin (et. other) addresses and data for evidential use.

Now when we know how to access ledger wallets, we need to study how to do a seizure from it.

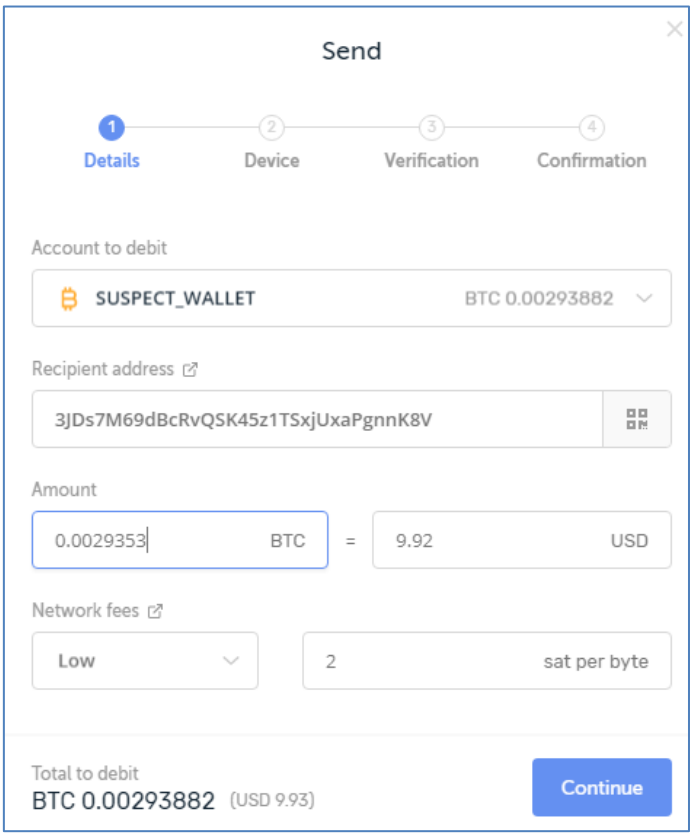
The first step is to create a government-controlled wallet and send our Bitcoins to it that we have already covered in earlier topics.



From the ledger manager we will select our Bitcoin account and select "Send".

It will ask for the destination of the Bitcoins here but with some modifications you can use this to any virtual currency.

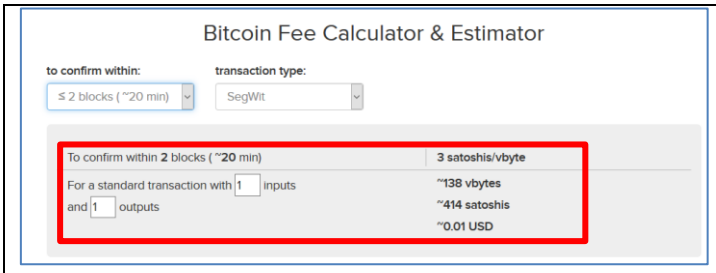
As mentioned before, one good practice when confiscating Bitcoins is to write the recipient address to a notepad by 2 or 3 separate persons and check that all written addresses match and after that put the address into the recipient address column. In the example I will send the Bitcoins to the address they were received from.



When doing a confiscation/seizure, it is recommended to use a very high transaction fee especially if you are transferring a big sum, you do not want to wait overnight or a few hours for it to be confirmed, it can be quite nerve wrecking.

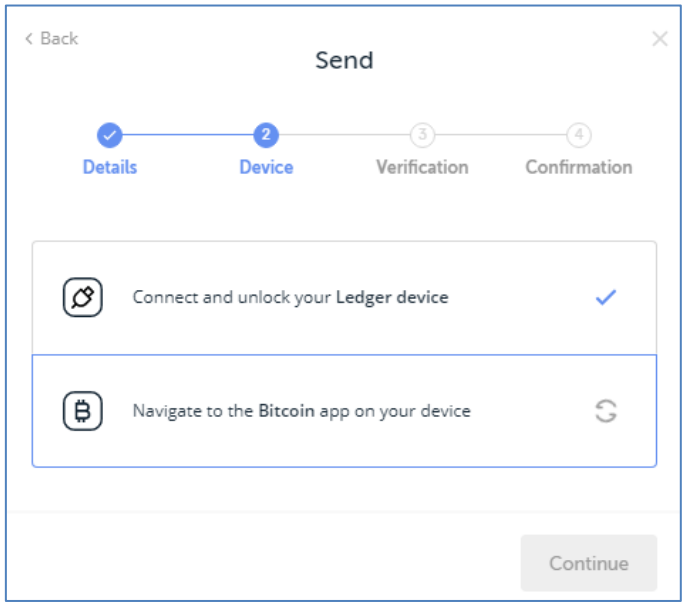
It is a good practice to check how many satoshis per byte is associated with what kind of delays for example from https://bitcoinfees.net/ or https://bitcoinfees.earn.com/

In the picture a one input and one output transaction in a SegWit transaction would be confirmed within 20 minutes with a fee of 3 satoshis/byte. From this we can estimate that there is not much traffic and delay in the network now and proceed with a quite low 2 satoshis per byte fee. This will make the



transaction go through the network within an hour. Since this is an exercise transaction, the fee is set quite low but when confiscating hundreds of thousands of euros or dollars, a 10 dollar or euro fee is nothing.

Once you have calculated and estimated the fees and given the seizure address to confirm the transaction, you need to connect and open the Ledger device again.

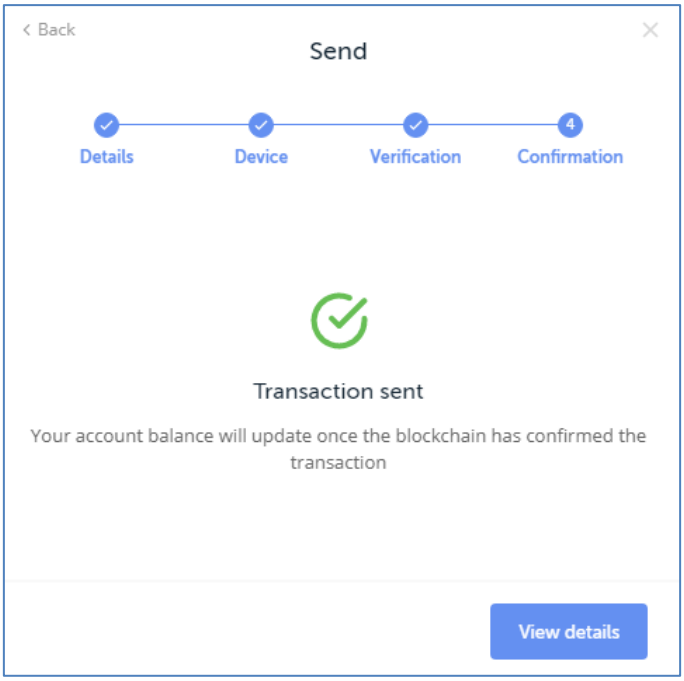


DO NOT press the right button before you have double and triple checked everything; confirm the destination address at least by two separate persons and make sure about the amount, and transaction fees attached to the transaction.

Immediately after you have confirmed the transaction by clicking on the right button the transaction is being sent to the destination address.

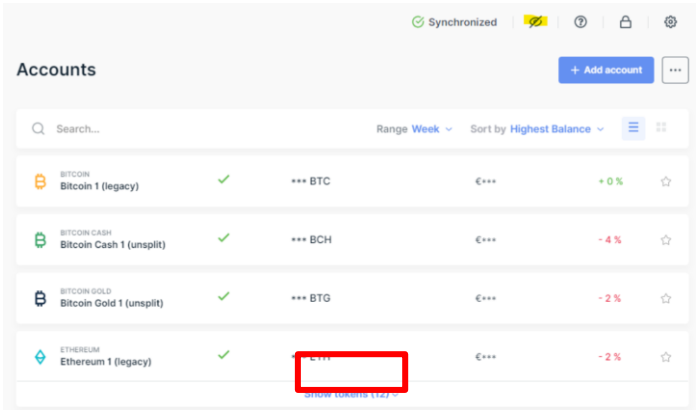
All done, if you followed the instructions you have now successfully confiscated or seized Bitcoins from a "suspects" hardware/software Bitcoin wallet.

You can apply all the same techniques to almost any wallet software or device. It is highly recommended to try out the Bitcoin Testnet to get familiarized with sending and receiving transactions



Seizing Ethereum ERC-20 tokens from a ledger device

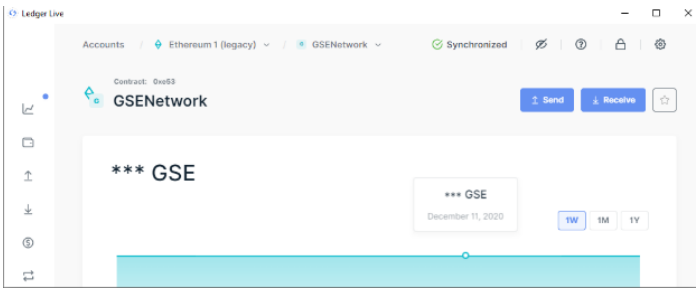
In the following example we found that the Ethereum wallet holds an ERC-20 token called GSE, which is the native token of the GSEnetwork[31,32].

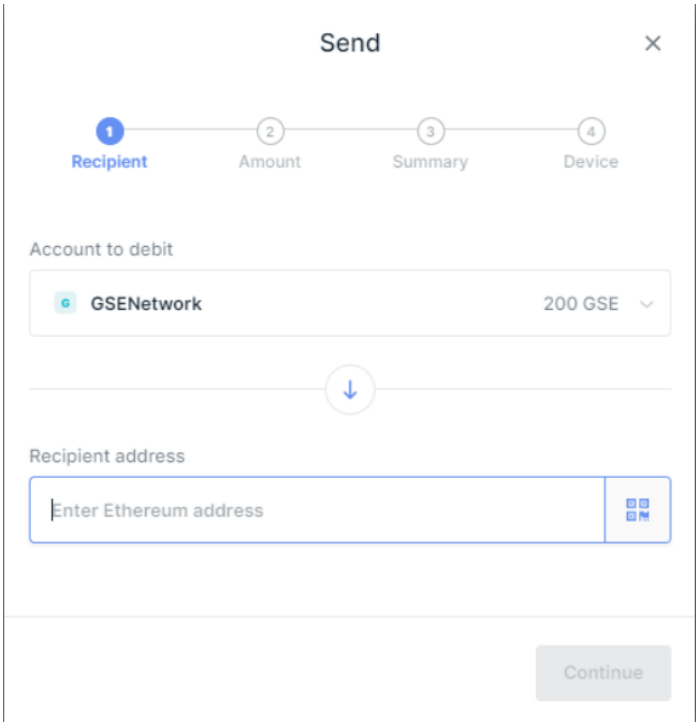


It can be seen when you install the Ethereum app on the ledger, in the example some of the details have been anonymized

The process of seizing ERC-20 tokens is a bit different than seizing bitcoins with some similarities to it. Main difference is when you transfer ERC-20 tokens from a Ethereum contract you make the transfer in the Ethereum network sending the content/tokens from one Ethereum

[31] https://cryptobriefing.com/what-is-gsenetwork-introduction-to-gse-token/
[32] https://etherscan.io/token/0xe530441f4f73bdb6dc2fa5af7c3fc5fd551ec838





contract to the government-controlled (Ethereum) contract.

One Ethereum address can hold several different types of tokens. The GSE Token contract address is seen in the below picture highlighted red box.

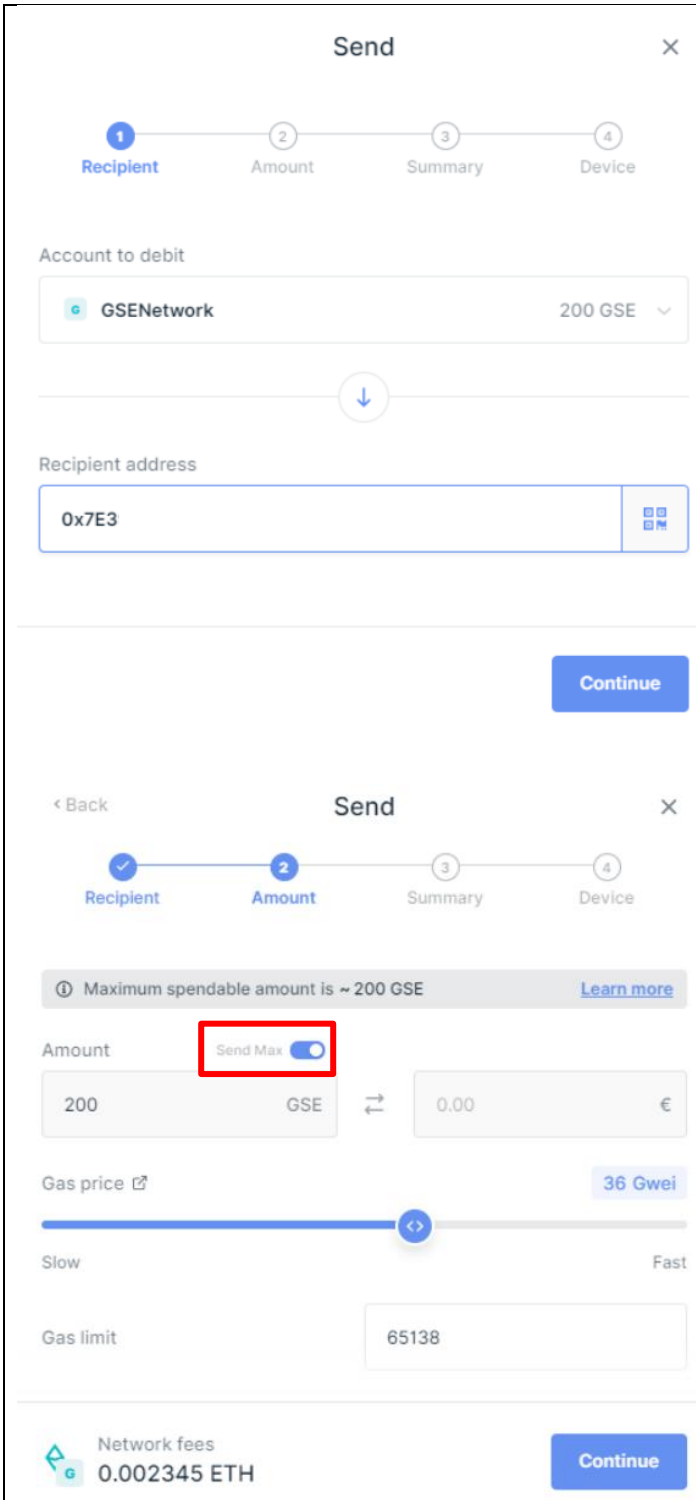
Making a seizure transaction from the GSE tokens we you need to select the token account from the Show Tokens highlighted in the picture in order to debit and add the Ethereum address we want the GSE tokens to be sent to.

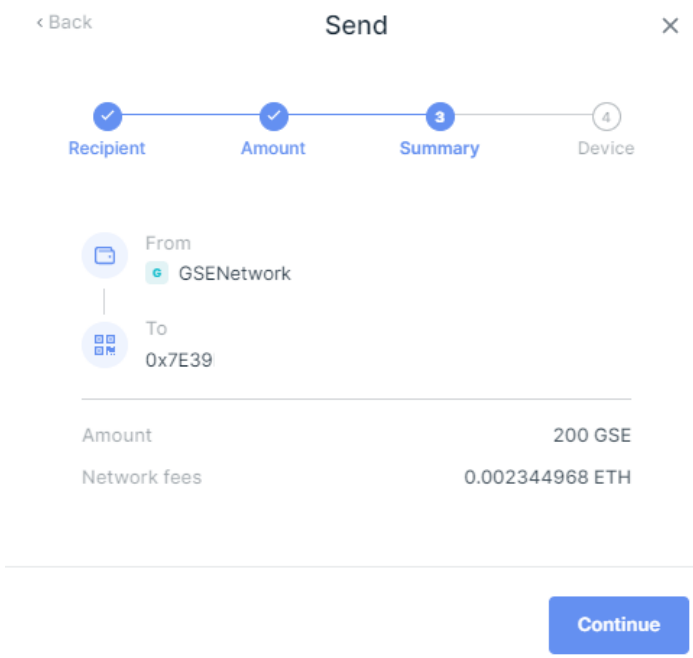
As mentioned before, some of the details are anonymized and hence the Ethereum address is not the full length in this example.

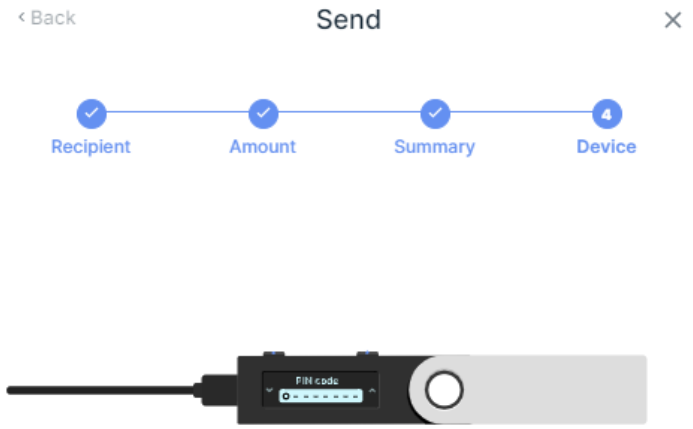
After pasting the Ethereum address we need to select the amount of Gas we want to associate with the transfer (Gas is Gwei and is equivalent to the bitcoin transaction fee which goes to the miner, Gwei being a fraction of Ether, like Satoshis in bitcoins). Also, the Ethereum network has gotten much slower and congested so the amount of Gas/Gwei to be used has gone up for the transactions[33,34]

Once we have determined the amount of GSE or by selecting Send Max that will be sent and set the destination Ethereum address with sufficient amount of Gas we can proceed to the transaction. Ledger software is very helpful and guides you through the process in many ways. It is still recommended to train different transactions with different cryptocurrencies, tokens, and other functionalities.

[33] https://ethgas.io/
[34] https://ycharts.com/indicators/ethereum_average_gas_price


Send
1 Recipient
2 Amount
3 Summary
4 Device
Account to debit
GSENetwork
200 GSE
Recipient address
0x7E3
Continue
Back
Send
Recipient
Amount
Summary
Device
Maximum spendable amount is ~ 200 GSE
Learn more
Amount
Send Max
200
GSE
0.00
€
Gas price
36 Gwei
Slow
Fast
Gas limit
65138
Network fees
0.002345 ETH
Continue

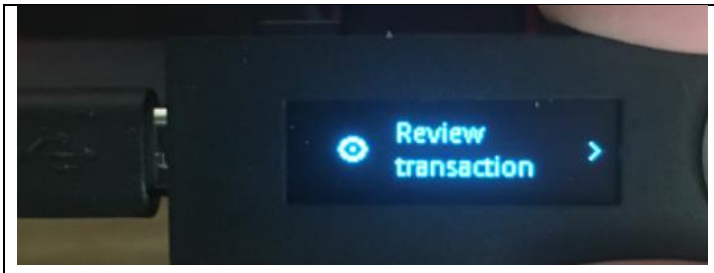




Ledger will ask you for the PIN code you entered earlier when restoring the device from seed words or by accessing the ledger live directly on the suspect computer or even with having the PIN code gotten from the suspect and with a clean installation of Ledger live. Then, you need to go to the Ethereum app that you have installed on the device.

Connect and unlock your device

In the ledger device and app you need to manually verify and review the transaction and double and even triple check that everything is correct. It is a bit difficult since the Ethereum address is quite long and you will need to scroll the screen to left or right. You will see an indicator like 1/3 of the page you are on.



Once you have reviewed and are certain that everything is correct and have a colleague checked it also, then you can proceed to send the transaction by clicking the top left button on the ledger unit and seize the GSE tokens.

3.6 Paper Wallet

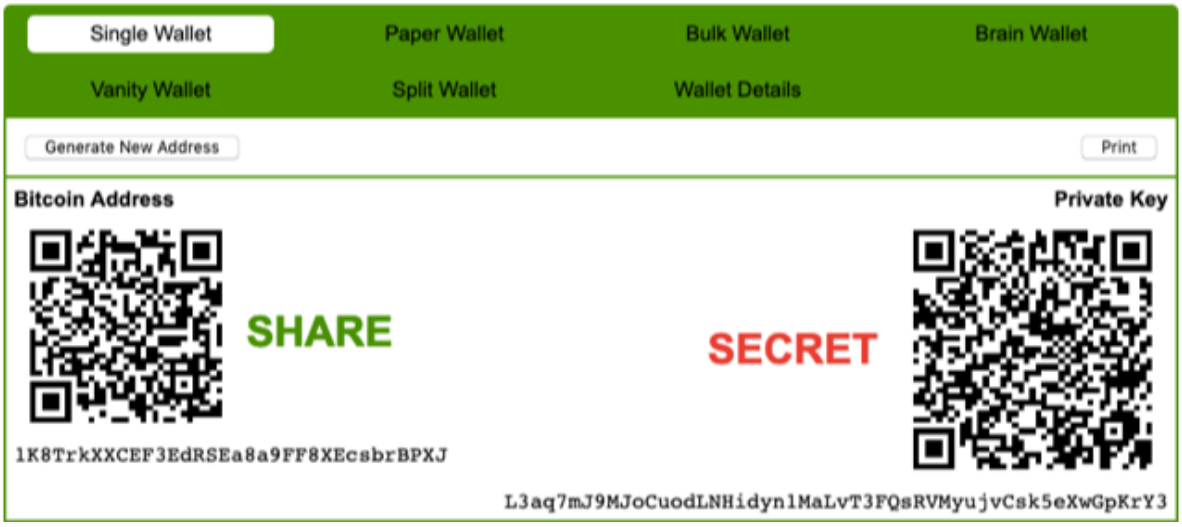
3.6.1 Introduction

Paper wallets were "a thing" in the early days of Bitcoin. They were mostly used between 2011 and 2016 when companies such as Trezor and Ledger were not very known in that time as they were just founded or starting up.

That does not mean that bitcoin paper wallets are not in use today, they could be waiting to be found somewhere hidden in a drawer or between a book.

Below is a screenshot of a bitcoin paper wallet. These paper wallets can be created online on the website www.bitaddress.org. However, the website advises to download the generation script and create a bitcoin wallet on an offline (by preference freshly installed) computer.

The generation script can be downloaded from their GitHub https://github.com/pointbiz/bitaddress.org/archive/v3.3.0.zip.



A typical paper wallet has one private key and one bitcoin address.

Paper wallets can also be encrypted. An encrypted private (bitcoin) key starts with 6P.

An example of an encrypted paper wallet is showed below.

In that case, investigators can only seize the funds when they know the password.

There are many possible ways to create a safe offline wallet. Some agencies have gone the way that they have a government wallet controlled by a virtual currency exchange, some have hardware wallets (demonstrated earlier), some have their own paper wallets with multi-signature keys.

The final demonstration is how to create an offline paper wallet with multi-signature. In this way there is a minimal possibility for hack or revealing your investigation to an outside exchange.

First you need to create a bootable Ubuntu DVD. You can download the Ubuntu image from the Ubuntu website. Following the download, you will then install the Ubuntu and a copy of the downloaded bittaddress.org copy on the DVD. Since the bootable DVD cannot be altered and the content can be verified with a SHA calculation, it can be considered quite tamper-proof. The most important thing when creating an offline wallet is to really be offline. Use devices that can be securely erased or use a totally separate dedicated computer. The wallet needs to have a chain of custody, when using multi-signature wallets even printing the public key on top of an evidence bag and the private key within a tamper-proof bag is a possible solution. There are several different ways to go, and the needs of the organization also have to be addressed. **When creating confiscation wallets, never use a network copier or printer to print the private keys or seed words!** Most of the network printers or copiers have a hard drive that stores the print buffer and therefore can be compromised as easily as the copy machine serviceman comes in and replaces the hard drive during normal maintenance.

In bitaddress.org offline code there is also a possibility to create a multi-signature wallet with a "master seed" and add one more point of protection. A typical wallet takes less than 1 minute to create and if printed with a printer that can either be destroyed or securely wiped, it is somewhat safe to use. For long-term storing, relying on one public – one private key combination is not recommended.

Many times, if you are in a hurry and need only a temporary holding for the bitcoins, you can either use a mobile app sweep wallet or create a few public – private key sets. To create a single address, you just open the Bitaddress html file in your DVD and move the mouse around until the counter hits 100 %.

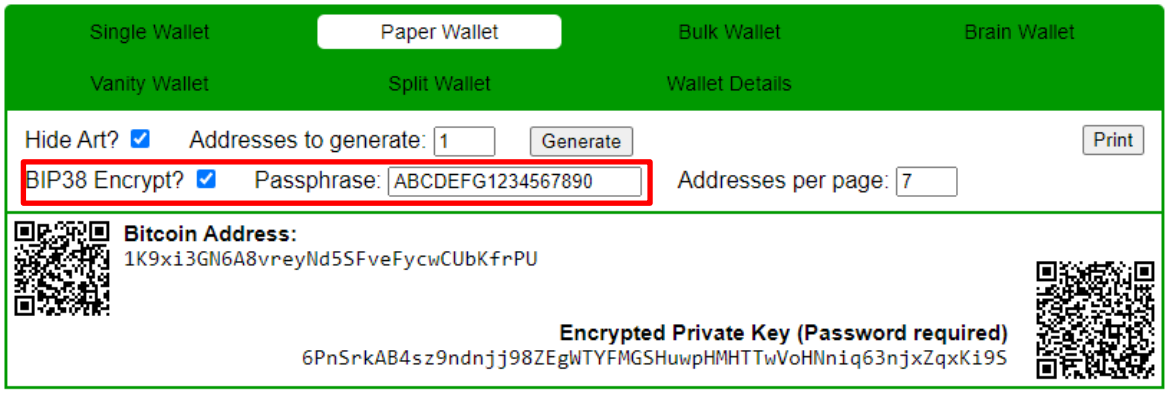
English | Español | Français | ελληνικά | italiano | Deutsch
Česky | Magyar | 日本語 | 简体中文 | Русский | português
bitaddress.org
Open Source JavaScript Client-Side Bitcoin Wallet Generator
95% 95% 95% Brain Wallet
95% 95% Wallet Details
Generating Bitcoin Address...
MOVE your mouse around to add some extra randomness... 95%
OR type some random characters into this textbox.
e4509121a399eb4b5d6b7098e0798d89fa0077e679e4c5967ab050ede4374b401a34a95
f687a096af51c74a78d4a8307f56bc6e95c41b18c13f76724c38c1198b4d38a9334c5d2
9e720ee253add2746cd2ace01271ca5941520467 8bac249291981e4c77a5c58ddc11c02
d6493aff203661c6e77e2850f4f297361f363075e07e6565e238665fd6f1caccd28ec1d
7cf7338ace4ea4b9b12570eedbb0bbb222f5a9438e38735d63e448386b52896a4f3c236
ba361c2676eab7ece9f194b7532e1b6cb58b46533e6f4c7ec8f7ba37a132a1b039797d7
63f6bb102cea317b3cffbf8a7cb42600122e1f99135b3e3a80f7eea9a42472e05cc2d92
ed530040c7e23c7
Donations: 1NiNja1bUmhSoTXozBRBEtR8LeF9TGbZBN
GitHub Repository (zip)
Version History (3.3.0)
527B 5C82 B1F6 B2DB 72A0
ECBF 8749 7B91 6397 4F5A
(PGP) (sig)
Copyright bitaddress.org. JavaScript copyrights are included in the source. No warranty.

Once you hit 100%, it will automatically create you a P2KH address which starts with a number 1. Something very important to remember is that it also creates the private key which must be considered a very secretive item. If anyone can see the QR code or the private key, they can withdraw the funds from the address. Also, after printing the public – private keypair remember to erase or wipe the printer memory.

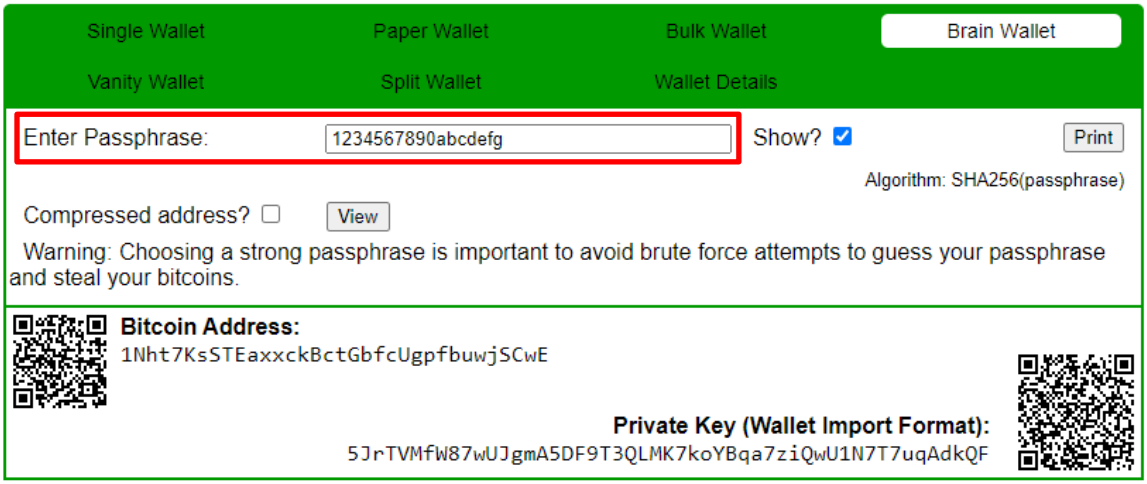
Creating a split wallet using bitaddress.org's script is a very easy process. Selecting the number of shares needed to combine and the number of shares that will be generated takes no time at all and now you have a multi-signature wallet. Below an example of an offline wallet consisting of three shares, any two of which can together sign transactions for the wallet.

3.6.2 Encrypted versus Non-Encrypted

For an additional layer of security, paper wallets can also be encrypted. When creating your organizations confiscation process, it is good to keep in mind since it can create another level or layer of security to the address your organization is using. However, is important to keep in mind if this master password is lost, it is close to impossible to brute force the password. This has been seen even with criminals that have lost their encryption master password and thus have also lost their funds.



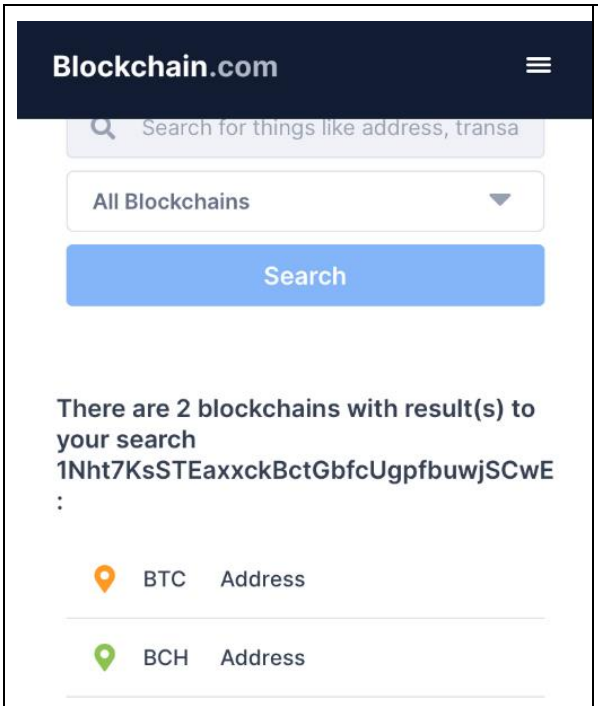
One way is also to create a Brain wallet, by remembering the passphrase, the encryption will always give you the same public and private key. When creating the passphrase wallet, it's good to be aware that for some common words there are bots scanning the Bitcoin network for these words, hashes, public and private keys. When the bot finds a wallet with funds, they immediately sweep the wallet and empty it. Bitmex published a report on a test they did and found out that it takes about 0.67 to 3 seconds to the wallet be emptied when using a commonly known passphrase[35].



Seizing a paper wallet

First step is to check on the blockchain if there are any funds to seize. Scan the QR-code next to Bitcoin Address on your mobile phone, copy it and browse to a bitcoin block explorer like www.blockchain.com/explorer.

[35] https://blog.bitmex.com/call-me-ishmael/ - interest piece, study on sweeping of brain wallets



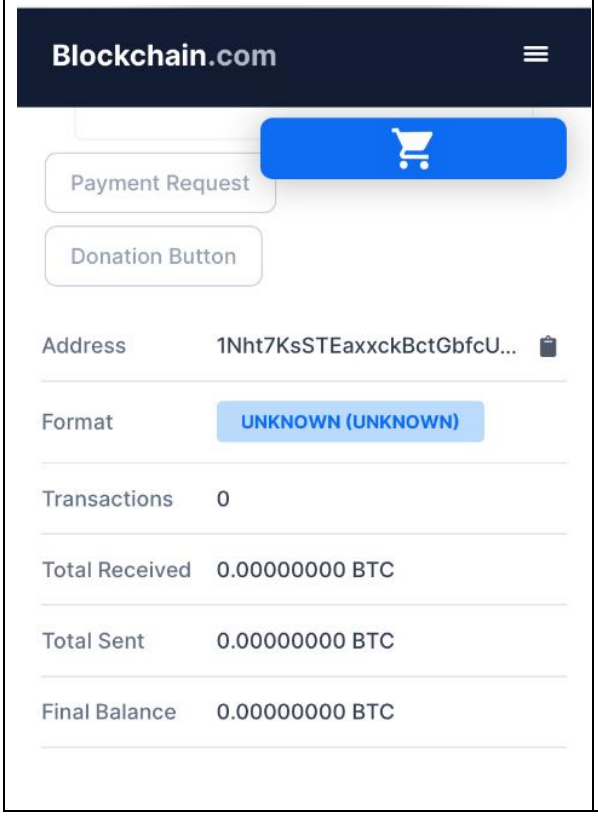
Paste the address in the search field.

You will see there a two potential blockchains with possible results: Bitcoin (BTC) and Bitcoin Cash (BCH).

First, click and check the Bitcoin (BTC) blockchain.

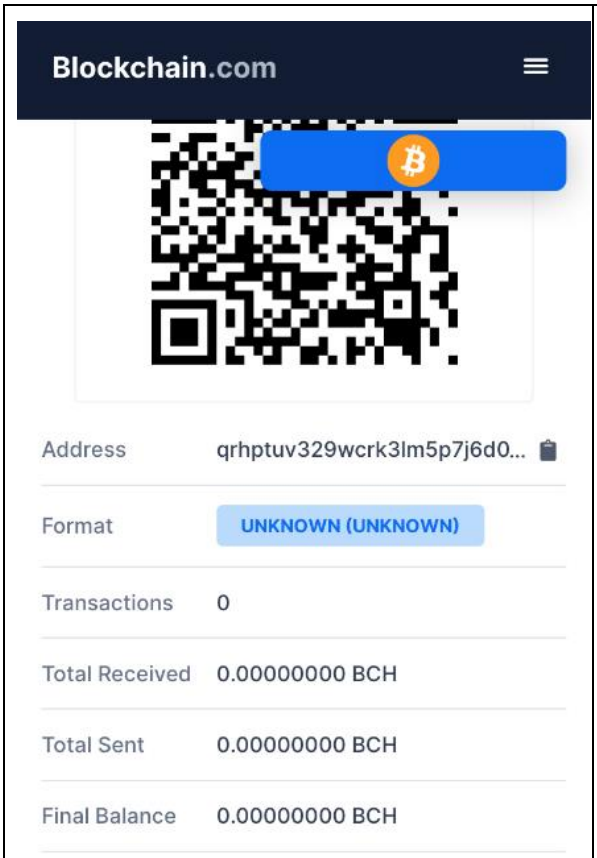
More info on the Bitcoin Cash fork can be found on: https://en.wikipedia.org/wiki/Bitcoin_Cash

More on Bitcoin forks can be found at: https://en.wikipedia.org/wiki/List_of_bitcoin_forks



Apparently, there are no bitcoins on this paper wallet as there are zero transactions and a final balance of zero as well.

Go back to the previous page of the explorer and click on Bitcoin Cash (BCH).

	Neither does the Bitcoin Cash blockchain show any funds. It means that this paper wallet is empty and never has been used.

Funds on the wallet?

To withdraw or seize bitcoins that are connected to a paper wallet, the best way to do is to use the "sweep" feature in a software wallet (mobile or desktop).

Sweeping

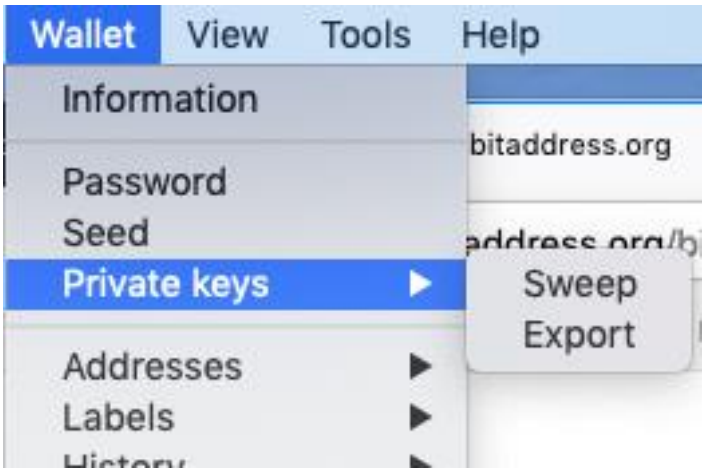
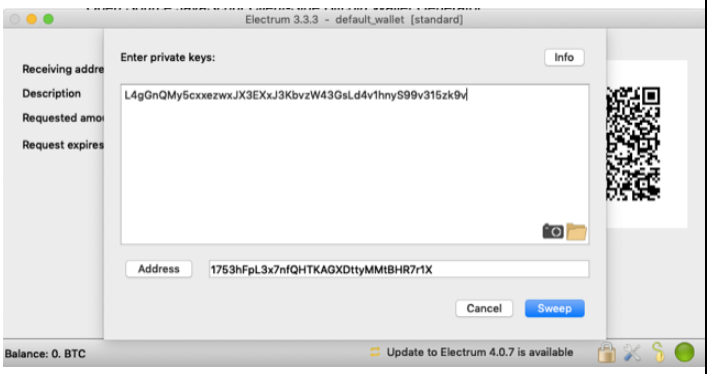
Sweeping the private key of the paper wallet will send the entire balance of this wallet to the wallet used and controlled by the government (or investigator).

In other words, the balance of the paper wallet address will be emptied and added to the government wallet. This happens through a standard transaction (that also requires the miner fees to be paid) so the wallet will have to be online (internet connection required).

One could also use an "import" function in a software wallet, but this is not a recommended practice as the investigator should perform a second manipulation, namely a transaction to a government-controlled wallet address. It also takes extra time and when an accomplice of the suspect also has a copy of the wallet, he/she could transfer the funds before the actual seizing took place.

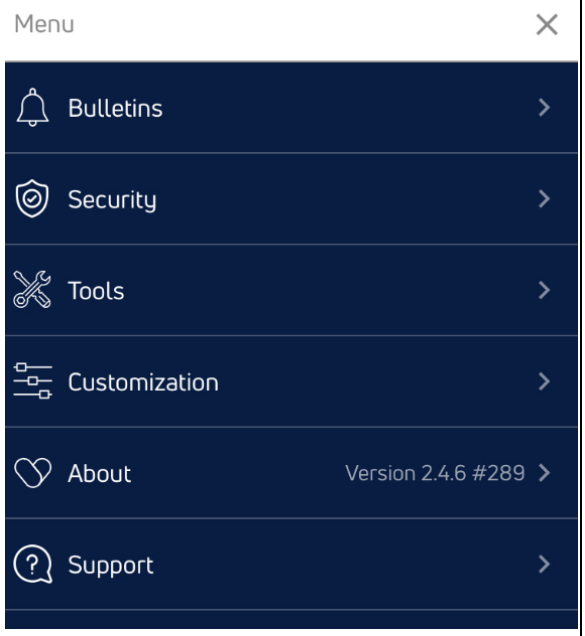
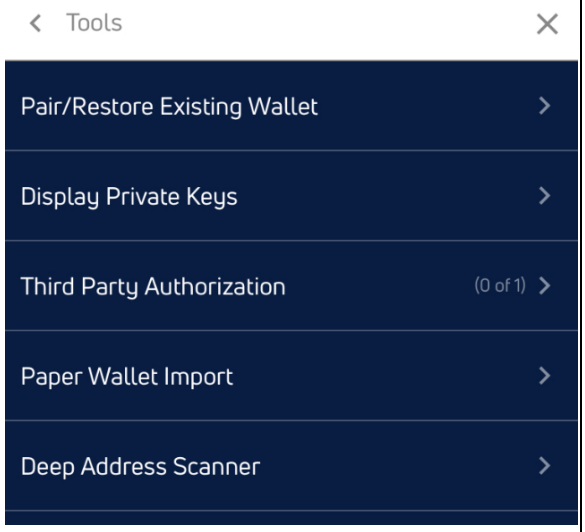
Sweeping a private key can be done in several wallets. Electrum, Mycelium and Jaxx Liberty (a mobile wallet) are supporting this. Jaxx Liberty mentions "import paper wallet" but rest assured, the wallet does a swipe.

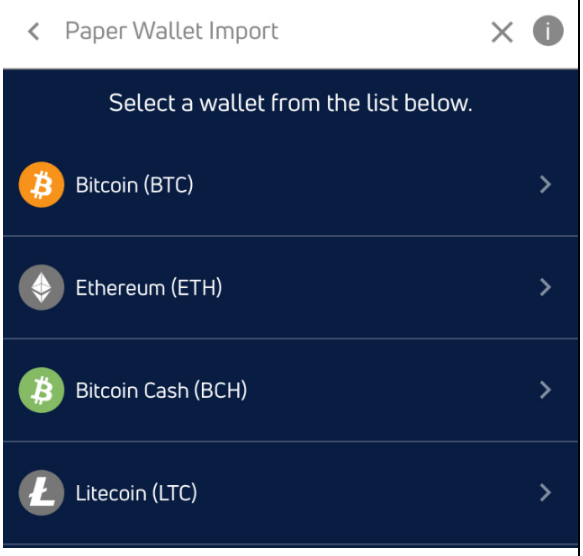
Sweeping of a bitcoin (BTC) private key in Electrum (desktop app)

	For example, sweeping an unencrypted private key can easily be done in a desktop wallet like Electrum. First, scan the QR of the private key on the paper wallet. Go to the Menu and click Wallet. Next, click Private keys and click Sweep.
	A new window will appear in Electrum. Copy and paste the private key in that window and click Sweep. You can copy it via a QR-code reader. Electrum will show you the address where the funds will be sent to (in the Electrum wallet).

Example sweeping of a Litecoin (LTC) private key in Jaxx Liberty (mobile app)

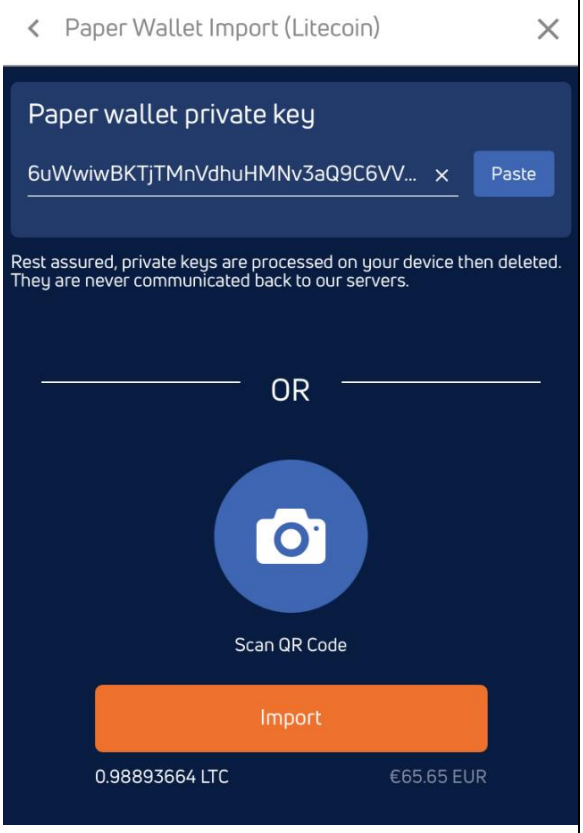
	Click the round/wheel icon (top right) in Jaxx Liberty.

	Next, click Tools.
	Next, click "Paper Wallet Import". Keep in mind it says: "import" but what Jaxx Liberty really does is a sweep of the private key.



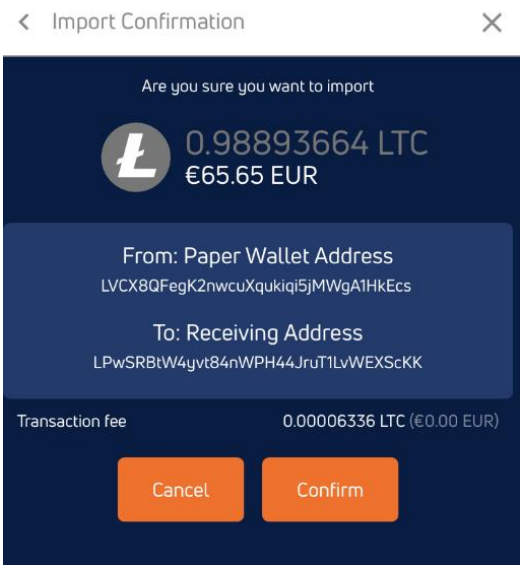
The next step is choosing what type of paper wallet you would like to import (sweep).

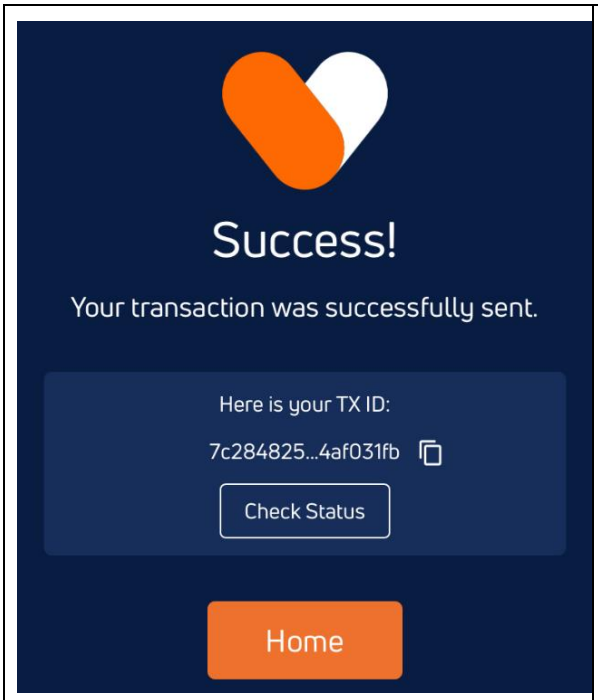
Click on Litecoin (LTC).



(left) Paste the private key or scan the QR code of the private key on the wallet.

(below) Click Confirm.



	If successful, the transaction ID will be presented. This you can copy somewhere to use later in the report.

3.7 Custodial and online web wallets

3.7.1 Introduction

A custodial wallet is a wallet where a third party is handling the key management, in many cases this third party will be considered a VASP (e.g., CoinBase, Xapo, BitGo).

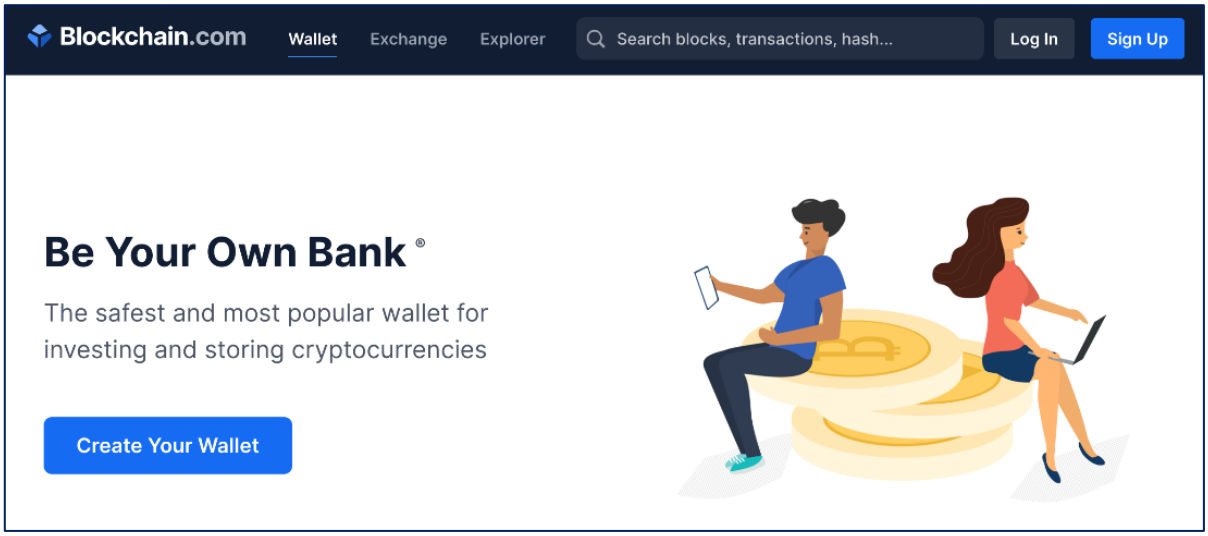
Institutional investors, such as banks, credit unions, insurance companies, pension funds and hedge funds also make use of custodial services.

In that regard, such a wallet can be considered as an online wallet but not all online wallets are custodial wallets. The private keys of these non-custodial online wallets are controlled by the user itself or by a combination of the user and the wallet provider. In that situation is a wallet like Block.io.[36]

Blockchain.com

An example of an online wallet that is not custodial is Blockchain.com wallet (which also exists as a mobile application).

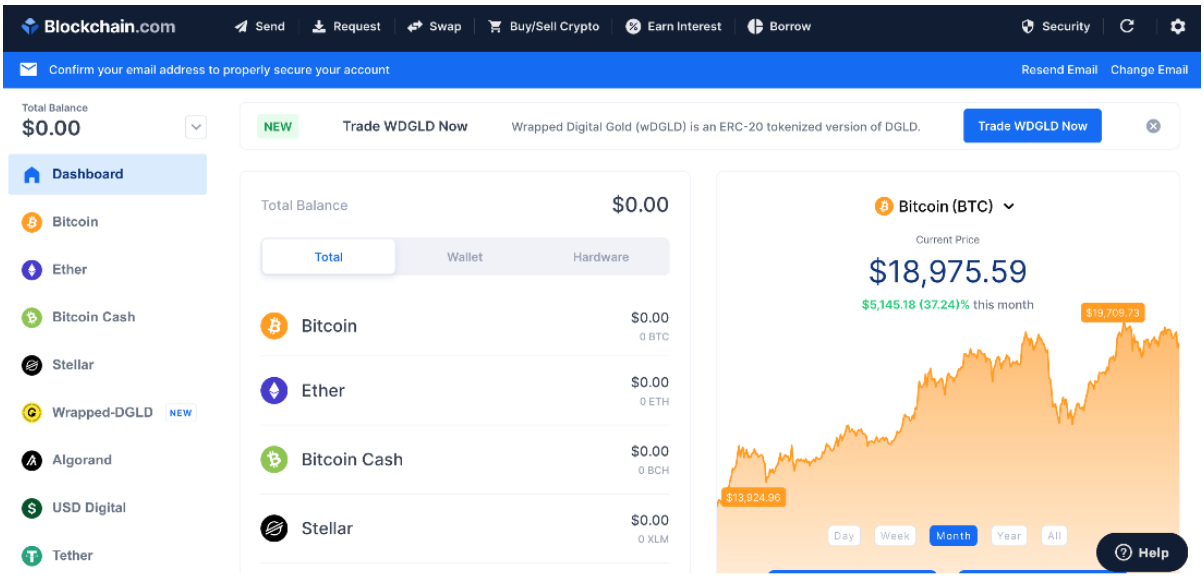
[36]Additional information https://block.io/security



The Blockchain.com wallet has a wallet identifier (Wallet ID) and a password to log in. This wallet ID is composed of 32 alphanumeric characters and 4 dashes, and takes the following format:

xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

When a user is signing up for a Blockchain.com wallet, he/she receives an email that contains his/her wallet identifier.



Just like most wallets, the Blockchain.com wallet also works with a (12-word) seed phrase.

Pre-seizure planning

When you think you are dealing with a custodial wallet, keep in mind the pre-seizure planning as explained before and contact the custodian (the platform) to freeze the account of that user.

It is good to know that the company Blockchain.com is unable to freeze user accounts or funds since they are not a custodial service. Other VASP's however, can do this if the law enforcement agency sends

them a subpoena, a warrant or MLAT depending on the applicable legal procedure which takes place. Usually there is a "for law enforcement" subpage for smooth cooperation.

Seizing

Seizing from the wallet itself can be a bit tricky. Investigators should keep in mind the following things (+ always check your applicable legal framework if allowed)

- The easiest situation is either when the suspect's wallet is open, or when the seed is found (for example during a house search). In this case, the investigator must secure the assets by transferring the funds to a government-controlled wallet.
- If the suspect's wallet is locked, but his/her email account is accessible, the wallet's password can be changed to gain access to the wallet. In this case, the investigator must have a legal authorization.
  In most cases, when creating an online wallet, an email account is necessary to verify the user and to authorize log in attempts.
- The wallet ID will also be mentioned at the bottom of the verification email.
- Approval of magistrate/judge/prosecutor is necessary to access the connected email account (depending on legal framework).
- Having all this information, the investigator could take over the wallet and transfer the virtual currencies to a government-controlled wallet.

Conclusion: the ideal seizing situation is when the wallet is open, or the seed was found. In most cases, the seed will be compatible with other BIP44/BIP39[37] type wallets, like Coinomi.

Know Your Customer information and contacting Blockchain.com (Luxembourg)

Blockchain.com (Blockchain Luxembourg SA) requires an identity verification of users who want to swap cryptocurrencies or take part of airdrops via their wallet.

This means that if law enforcement finds an address (Bitcoin or other cryptocurrency) or a transaction hash value, then Blockchain Access UK Ltd. can correlate it to the user's profile if the address or hash was used in a swap or exchange transaction (since KYC is needed for these actions). This subsidiary of Blockchain.com handles the exchange, institutional custody, and over-the-counter trading services.

Blockchain Access UK Ltd. operates as an exchange and is "*a registered Money Services Business in the United States. As such, it collects and records customer information consistent with the risk-based approach required by, e.g., the United States Bank Secrecy Act.*"

As indicated above, Blockchain.com stores data of its customers, and if officially requested, they must share it with law enforcement officers.

However, according to their website, Blockchain Luxemburg does not know following information of their self-custodial wallet users.[38]

- Wallet balances
- Transaction history
- Explorer pages visited
- Legal names

[37] Refer to https://www.blockplate.com/blogs/blockplate/list-of-bip39-wallets-mnemonic-seed for a list of compatible wallets.

[38] More info at: https://www.blockchain.com/legal/law

- Mailing addresses
- Social security or national ID numbers

It is worth to underline that even though the EU regulation, Blockchain Luxembourg stated that they cannot spend virtual currency on a user's behalf (or against the user's wishes), freeze or forfeit virtual currency on law enforcement's behalf, or know the contents of wallets.

3.7.2 Best practices and guidelines

Investigators might find interesting leads when looking into the browser history of their suspect. Leads might pop up to Virtual Asset Service Providers where they are doing their money laundering or are storing their illicit proceeds for example.

Another important step is to check the 2FA applications on suspects smartphones. Do they have a Google Authenticator link with Kraken or others? If so, chances are they are holding an account on that platform.

Good to know is that practically all custodial wallets (especially cryptocurrency platforms) have personal information on their users. At least, they will be able to share an email address and IP address logs.

When individuals want to trade above a certain amount or if they want to trade with fiat money, chances are that they must comply with the Know-Your-Customer (KYC) regulation of the platform they are conducting business on.

Let us look at Kraken[39,40] for example. Kraken is known to have very good know your customer policies that can help law enforcement identify the persons behind the virtual currency transactions to and from their service.

[39] https://support.kraken.com/hc/en-us/articles/360001449826-Deposit-and-withdrawal-limits-by-verification-level
[40] https://support.kraken.com/hc/en-us/articles/201352206-Verification-level-requirements

	Daily limits	Monthly limits	Margin	Requirements
Tier 0 Deposits and withdrawals are not available.	Deposit (fiat) ..... $0.00 Deposit (crypto) ..... $0.00 Withdraw (fiat) ..... $0.00 Withdraw (crypto) $0.00	Deposit (fiat) ..... $0.00 Deposit (crypto) ..... $0.00 Withdraw (fiat) ..... $0.00 Withdraw (crypto) $0.00		Account signup
Tier 1 You can trade between all currencies, but account funding is limited to digital currencies only.	Deposit (fiat) ..... $0.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $0.00 Withdraw (crypto) $2,500.00	Deposit (fiat) ..... $0.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $0.00 Withdraw (crypto) $20,000.00	Enabled	• Full name • Date of birth • Country of residence • Phone number
Tier 2*	Deposit (fiat) ..... $2,000.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $2,000.00 Withdraw (crypto) $5,000.00	Deposit (fiat) ..... $10,000.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $10,000.00 Withdraw (crypto) $50,000.00	Enabled	• All of the above • Address verification
Tier 3	Deposit (fiat) ..... $25,000.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $25,000.00 Withdraw (crypto) $50,000.00	Deposit (fiat) ..... $200,000.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $200,000.00 Withdraw (crypto) $200,000.00	Enabled	• All of the above • Government issued ID • Verified proof of residence (e.g., utility bill no more than 3 months old) • Social Security number (US only) • ID confirmation photo (see footnote)*
Tier 4 Individual High Value Account *or* Corporate Account	Deposit (fiat) ..... $100,000.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $100,000.00 Withdraw (crypto) $100,000.00	Deposit (fiat) ..... $500,000.00 Deposit (crypto) ..... No limit Withdraw (fiat) ..... $500,000.00 Withdraw (crypto) $500,000.00	Enabled	• If you are interested in a personal or business Tier 4 account, please contact support. • Choose the category "Verification: Tier 4" for your support request.

Proper KYC ensures that the platform should have at least the following documents available for law enforcement upon request:

- Verified name with driver's License or government-issued photo ID
- Verified proof of residency
- Social security number
- Email, phone number

- IP and Cookie information

A Virtual Asset Service Provider can be contacted via various channels to know if they have KYC-information on a specific user. Before making initial contact, it is good to consult your LEA community to check if the Virtual Asset Service Provider is compliant. If they have KYC and other relevant information, investigators need to send a subpoena or depending on jurisdiction appropriate request to obtain this information.

3.7.3 Two-factor authentication (2FA)

Users are encouraged to use 2FA (via Google Authenticator, YubiKey, Authy or SMS codes). In many cases, as an extra security layer, a link will be sent to the connected email address when the user wants to login. So even when an investigator has a password and access to the authenticator app, access (with approval of the magistrate/judge - see above) to the email account of their suspect could also become necessary.

3.8 Seeds

Seed words are discussed in this manual several times, it is an important and essential part of cryptocurrencies. With the seed you can restore and seize a multitude of different coins and restore the exact same copy of the suspect's wallet.[41] However, it is also important to know that some of the wallets do not follow the BIP protocols in the same manner and hence one wallet can return you a bunch of coins whereas another opens a completely empty wallet.

To investigate the seed words there are some tools to determine the private keys even without a cryptocurrency wallet installation. As pointed out earlier, BIP32/44/49 wallets should give out the same addresses, but this is not always the case[42]. Electrum, Exodus, Mycelium, Copay, Jaxx, Coinomi and some other wallets can return a totally different set of private and public keys. This is because different software providers use the seed algorithms a bit differently. Therefore, it is recommended to try different restoration processes and tools. Ian Coleman has created a website called Mnemonic Code Converter[43] which can be downloaded offline to check which addresses are associated with seed words, however it does not seem to recognize the difference and analyze what keys different software returns. It is still very useful, and in the converter, you can use seed words of many different virtual currencies. It is recommended to test and try out these derivation tools available, also there might be some specific law enforcement tools available in your agency.

When checking the seed words (BIP49) that were used in this manual

"side useful wide unhappy gallery spoon exhibit cushion depth valid vibrant coach situates never device index awkward birth ankle spend appear party blast alley"

we will get the result for the key

Derivation path m/49'/0'/0'/0/0

Public key: 3A9XTNSSaQesZjDwEWcP6knKGC9YzFBQHe

Private key: L2HFbHMB3hZVsaVQDkD7D7VUKg8A96x7mKhazKGQreJLGUfApHhQ

[41] Further reference https://en.bitcoin.it/wiki/Seed_phrase
[42] Further reference of seed words https://walletsrecovery.org/
[43] https://iancoleman.io/bip39/

This is correct. So, in a way, you can also use this tool to generate the correct private keys from the seed word list. It is highly recommended to practice with these tools. The derivation path is created as follows[44]

m/purpose/coin_type/account/change/address_index

- m: is the master key
- purpose: is the BIP implementation, in this case 49 stands for BIP49
- coin_type: is currently 0 as for Bitcoin, 1 would be for Bitcoin Testnet, 2 for Litecoin and 60 for Ethereum
- account: gives the possibility to set up sub accounts for example 1 is for dirty coins and 2 is for mixed coins, and 3 could just be the clean coins etc.
- change: flags the address as an address purely to receive change from a transaction
- address_Index is a number representing the numbered receiving address for payments
- numbering: starts from 0, therefore the value 3 would be the receiving address 4 on that branch of the tree

When using a tool like the Ian Colemans derivation path tool, you do not actually need to install the same type of wallet to the computer that the suspect has.

3.9 Reporting

When seizing cryptocurrencies, some information needs to be documented and reported. The relevant information and the elements of the report depends on the country's applicable legal framework and reporting standards.

Regarding a seizing transaction, a report usually at least contains the following information:

- Name of cryptocurrency (e.g., Bitcoin, Ethereum)
- Amount (e.g., 0,15 BTC, 1 ETH)
- Transaction fee (amount)
- Date, time, and time zone (e.g., 25/12/2020 10:00 CET)
- Transaction ID (hash)
- Sender's address(es)
- Recipient address (i.e., government-controlled address)

Also, in the report you can specify what kind of wallet(s) and device(s) are used, in what circumstances and how the seizure was carried out, manipulations performed on the device(s), the balance when seizing, etc.

Never reveal private keys or seeds of a government-controlled wallet in a report.

When seizing bitcoins for example, the immutable blockchain of Bitcoin can serve as a form of indisputable evidence. Bitcoin transactions with their corresponding information are automatically recorded and thus documented in the public Bitcoin blockchain.

It is a good practice to add (a) screenshots and/or screen recording (without displaying of the private key) of a seizing transaction to the report.

[44] For more information on derivation paths refer to https://en.bitcoin.it/wiki/BIP_0175

4 Closing words

This manual was tasked and developed within the European Union iPROCEEDS-2 framework. It will give the investigator hands-on experience and guide to master some of the needed knowledge and TTP's to be able to seize cryptocurrencies. Unfortunately, due to the very extensive scope of this (seizing) area, not all topics could be covered.

All software and techniques were valid while writing the manual. However, the investigators need to be aware that the cryptocurrency field is continuous evolving and changing quite quickly. Therefore, once they are aware that they need to seize cryptocurrencies investigators also need adequate time to prepare and update themselves and train/practice beforehand.

Sometimes there are situations that cannot be expected but by testing and practicing the topics covered in this manual, it will be a big step forward to be successful in many situations.

It is also recommended to use available supporting material mentioned below:

- Europol Bitcoin investigation guide
- Guidelines for the Seizure and Sale of Virtual Assets, INTERPOL (November 2020, for official use only)
- "Cryptocurrency and Dark Web Investigations" training package (EMPACT – ECTEG)
- Nick Furneau Investigating cryptocurrencies[45]

This is a manual for government and law enforcement distribution only, unauthorized distribution and/or copying any part of the manual is restricted/denied.

[45] Nick Furneau Investigating cryptocurrencies: https://investigatingcryptocurrencies.com/